# REESTRUCTURACIÓN DEL PROCEDIMIENTO ACTUAL DE GENERACIÓN DE LLAVES DE CIFRADO PARA CAJEROS ELECTRÓNICOS

FREDDY ENRIQUE ACOSTA
IGOR ALEXANDER GOMEZ MARTINEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN DE SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2012

# REESTRUCTURACION DEL PROCEDIMIENTO ACTUAL DE GENERACIÓN DE LLAVES DE CIFRADO PARA CAJEROS ELECTRONICOS

FREDDY ENRIQUE ACOSTA
IGOR ALEXANDER GOMEZ MARTINEZ

Proyecto para optar el título de Especialista en Seguridad Informática

Director: Ing. JOSE ALFONSO VALENCIA RODRÍGUEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSTGRADOS
ESPECIALIZACIÓN DE SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2012

**Nota de Aceptación**

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C., 23 de Noviembre de 2012

## DEDICATORIA

Agradezco a mi madre quien en todo momento ha sido apoyo y consorte para cuanta meta me he propuesto. A mi familia por encontrarse presente a lo largo de esta larga carrera que hoy culmina y por último, pero no por esto menos importante, a mis amigos sin los cuales cada tarea y cada proyecto habían perdido el tinte de alegría y solidaridad que ustedes les dieron. A Dios, gracias.

**Igor Alexander Gómez Martínez**

A mi mamá Cecilia Acosta Oliveros por brindarme todo su apoyo, su entrega y confianza necesaria para sacar adelante el fruto de una especialización que se ve reflejada en metas que como este proyecto se logran alcanzar.

A mis hijos María Camila, Daniela Alejandra y Nicolás Andrés; porque son el motor de mi vida y han iluminado aún más el camino que empecé a recorrer como profesional y que día a día espero seguir superando, para ser el ejemplo de ellos y todos los que creyeron en mi y hoy no tengo palabras para decirles gracias.

**Freddy Enrique Acosta**

## AGRADECIMIENTOS

Freddy Enrique Acosta e Igor Alexander Gómez Martínez expresan sus agradecimientos a:

Msc Ing. Alfonso Valencia por su importante orientación metodológica en el desarrollo de este proyecto; donde debemos destacar su disponibilidad la cual sin duda alguna ha enriquecido el trabajo realizado.

Debemos agradecer de una manera especial y sincera al Dr. Pedro Díaz por los conocimientos transmitidos en las asignaturas orientadas los cuales han sido de gran ayuda para la elaboración de este proyecto.

Queremos expresar un sincero agradecimiento al Dr. Jesús Rodríguez Cabrero Director General de Realsec; por haber dado respuesta a nuestras peticiones a través de Linked in y habernos contactado con Sebastián Muñoz.

Queremos expresar nuestros agradecimientos al B. Sc. Ing. Sebastian Muñoz CEO & Founder at Realsec. Inc por su importante aporte y participación activa en el desarrollo de este proyecto. No cabe duda que su aporte he enriquecido el proyecto realizado.

**CONTENIDO**

pág

# LISTA DE TABLAS

pág

# LISTA DE FIGURAS

pág

# GLOSARIO

**ACCESO REMOTO**: permite que el usuario con su computadora interactúe con un programa en otra computadora a través de la red o Internet.

**CAJERO AUTOMÁTICO (ATM)**: es una máquina expendedora usada para extraer dinero utilizando una tarjeta de plástico con una banda magnética o chip (tarjeta de débito por ejemplo), sin necesidad de personal del banco.

**CIFRADO**: proceso de transformación de un texto denominado “texto plano” para convertirlo a una forma que no pueda ser leída por alguien que no tenga los mecanismos utilizados para llevar a cabo la encriptación. El texto transformado recibe el nombre de “texto cifrado”.

**COMPONENTE**: Corresponde a una de las partes que conforman el Criptograma.

**CONFIDENCIALIDAD**: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**CRIPTOGRAFÍA**: es la ciencia que estudia la escritura oculta, pero aún se puede precisar más este concepto, y así, esta disciplina, es entendida como el arte de escribir en un lenguaje convenido mediante el uso de claves, es decir, la criptografía enseña a diseñar códigos secretos.

**DISPONIBILIDAD**: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizadas.

**INCIDENTE INFORMÁTICO**: cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación.

**INTEGRIDAD**: propiedad de salvaguardar la exactitud y estado completo de los activos.

**IP (INTERNET PROTOCOL)**: etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

**ISP (PROVEEDORES DE SERVICIOS DE INTERNET)**: en Colombia estos entes brindan adicionalmente servicios de telefonía y televisión, convirtiéndose de esta manera en unos prestadores de servicios integrales de telecomunicaciones.

**LOG**: registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información

sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

**LLAVE DE CIFRADO**: es una secuencia de número y letras mediante el cual especifica la transformación del texto plano en texto cifrado.

**RIESGO INFORMÁTICO**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**SEGURIDAD DE LA INFORMACIÓN**: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, responsabilidad con obligación de reportar (*accountability*), no repudio y fiabilidad.

**SEGURIDAD LÓGICA**: consiste en la aplicación de barreras que resguarden el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas.

**TKE (Trusted Key Entry)**: dispositivo de seguridad basado en hardware que permite la generación segura de componentes de encripción.

# RESUMEN

El proyecto de "*reestructuración del procedimiento actual de generación de llaves de cifrado para cajeros electrónicos*", modifica la forma de generar los componentes necesarios para la activación de los servicios del cajero y con esto mitigar el fraude presencial en los ATM's; logrando con esto la confidencialidad, integridad y evitar el repudio de las transacciones electrónicas.

Para el desarrollo de la reestructuración del procedimiento de generación de llaves de cifrado se toma como referente el proceso que se lleva hoy en día; con base en este planteamiento se caracterizan cuatro (04) alternativas de solución (Futurex Series RKMS, Cryptosec-RKL, ProRKL Wincor Nixdorf y EFTSec); las cuales proporcionan una visión clara para el diseño del nuevo procedimiento de generación de llaves de cifrado de forma remota.

La alternativa de solución seleccionada debe cumplir con los mínimos estándares de seguridad expuestos en las circulares externas 052 de 2007 y 022 de 2010 emitido por la Superintendencia Financiera de Colombia y la norma de seguridad de datos PCI versión 2 de Octubre de 2010; así mismo debe ser un dispositivo multivendor que permita accionar con todas las marcas de cajeros a nivel nacional.

Para el caso de estudio se seleccionó la alternativa de solución Cryptosec-RKL que proporciona los dispositivos para la generación de las llaves de cifrado de forma remota; esta tecnología está basada en un HSM (Hardware Security Module), que suministra una protección de las llaves maestras; pero para hacer este proceso hace falta más que un HSM, para lo cual el Cryptosec-RKL tiene una completa aplicación software que reside en el dispositivo junto con el HSM; y permitirá instalar la licencia agente de forma remota en cada ATM sin importar el fabricante (Diebold, NCR, Wincor, etc) .

La implementación de la infraestructura con la alternativa seleccionada para el periodo 2012 – 2013 tiene un costo de USD 277.680 que deberán ser tomados en cuenta en el presupuesto anual designado por cada entidad financiera colombiana, así como las herramientas, acciones y procedimientos para lograr los objetivos planteados.

# INTRODUCCION

El proyecto de reestructuración del procedimiento actual de generación de llaves de cifrado para cajeros electrónicos, pretende modificar la manera como se generan los componentes necesarios para la activación de los servicios del cajero y con esto mitigar el fraude presencial[1] en los ATM's; logrando con esto la confidencialidad, integridad y evitar el repudio de las transacciones electrónicas.

Algunos de los estándares que gobiernan las políticas de seguridad lógica en lo que respecta a la gestión del PIN son los publicados y revisados por la Superintendencia Financiera de Colombia participado expertos de la Asociación de la Banca (ASOBANCARIA), quienes están a cargo de la revisión de estas especificaciones cada cinco (05) años para acomodar las tecnologías emergentes.

Las franquicias Visa y MasterCard definen técnica y procedimiento para transferir las claves por medio de su módulo de seguridad con el fin de preservar su integridad; así mismo, las franquicias anteriormente mencionadas utilizan el sistema tradicional para la generación de claves en claro; teniendo en cuenta que dichas claves se pueden ver comprometidas durante el proceso de carga se le exige a las franquicias el cumplimiento del principio dual control (que actualmente es el sistema diseñado de claves en componentes y el envío de éstos a los custodios por diferentes canales de comunicación).

No obstante, la compleja logística y la ineficiencia en los procesos manuales; y aplicando los requisitos de VISA, hace que el procedimiento de carga manual de claves en los cajeros automáticos se pueda llegar a traducir en una carga tediosa, expuesta a errores y con un costo elevado para el Banco.

Por lo anterior; y para cubrir las necesidades con la tecnología disponible de criptografía asimétrica, el áreawwwwwwwwwww de seguridad informática dentro del sector financiero promueven la revisión de estándares periódicamente para incluir nuevos procedimientos para la carga de los componentes definiendo un nuevo marco de seguridad por medio de criptografía de clave pública.

Es por esto que el nuevo esquema que se plantea en este proyecto tiene como objeto la carga remota de llaves de cifrado, la cual nos permitirá eliminar costos que se incurre en el proceso manual al suprimir la necesidad de desplazar personal para hacer el ingreso de las claves en el Cajero Automático.

[1] ESPINOSA RODRÍGUEZ, Francisco. Seguridad en operaciones financieras. Superintendencia Financieras de Colombia. Bogotá D.C. Agosto 2012. Disponible en Internet: http://www.sse.com.co/fraude-financiero-

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 PLANTEAMIENTO DEL PROBLEMA

El rápido cambio tecnológico por el que atraviesa el mundo contemporáneo, con los grandes avances en las tecnologías de la información y las comunicaciones (TIC), así como la biotecnología y los nuevos materiales, plantean una serie de oportunidades y desafíos a la sociedad y a la estructura productiva de los distintos países a nivel mundial. De esta forma, es común escuchar que aquellos países que no logren adaptar para sí las transformaciones impulsadas por las nuevas tecnologías en la industria, agricultura, salud, medio ambiente, energía, educación, y otros sectores, corren el riesgo fatal de quedarse a la zaga en términos de desarrollo y bienestar; y más aún en el caso particular de los países en desarrollo, de profundizar la llamada brecha tecnológica que los separa del mundo industrializado[2].

Por lo anterior, y para estar a la vanguardia de la tecnología el sector Financiero Colombiano ha implementado nuevos productos a sus clientes; para lo cual, han llevado a un sinnúmero de bancos a implementar entre sus servicios, los cajeros automáticos (ATM).

La red de cajeros automáticos permiten a los usuarios utilizar de una forma segura y confiable los diferentes tipos de actividades transaccionales ofrecidos por cada entidad bancaria como son: retiros, pagos de servicios, consultas de saldos, transferencias, entre otros; por tal motivo, este medio electrónico debe ser confiable para los clientes de la red quien los utiliza; por esta razón, las entidades financieras se ven en la necesidad de utilizar métodos de codificación para la protección de la información de acuerdo a las circulares externas 052 de 2007 y 022 de 2010 emitido por la Superintendencia Financiera de Colombia y la norma de seguridad de datos PCI versión 2 de Octubre de 2010.

Hoy en día en Colombia los cajeros automáticos, y tomando como referencia las circulares externas 052 de 2007 y 022 de 2010 la norma PCI, se deben realizar un intercambio dinámico de llaves entre los sistemas de cifrado con una frecuencia necesaria para dotar las operaciones realizadas; este proceso consiste en preparar una consola de ingreso de llaves; y por medio de dos (02) custodios

[2] RAMÍREZ DE RINCÓN, Marta Lucía. Tecnología e innovación: Impacto en la competitividad. Bogotá D.C. Abril 2010. Disponible en Internet: Biblioteca virtual Luis Ángel Arango http://www.banrepcultural.org/blaavirtual/ciencias/sena/cursos-de-capacitacion/politicanal/politica3.htm

hacen la generación e impresión manual de dos (02) componentes, y así formar la llave de cifrado para cada cajero automático; las cuales son guardadas en cofres de seguridad en cada oficina de la red bancaria para ser utilizadas cuando sean requeridas. Para el ingreso de las llaves se debe llevar cabo de forma manual por dos (02) personas quienes son el ingeniero de campo asignado por la marca del cajero y el subgerente de la oficina; de esta manera, el cajero queda habilitado a servicio de los clientes; sin embargo, las llaves de cifrado aún continúan en poder de las dos personas que efectúan el procedimiento.

## 1.2 FORMULACIÓN DEL PROBLEMA

Desde que las tecnologías de Información empezaron a ser parte importante en las operaciones de las compañías el tema de la seguridad ha venido tomando cada vez mayor importancia, derivando en un sinfín de soluciones y estándares como el Payment Card Industry – Data Security Standard (PCI-DSS). Se ha comprobado que la efectividad de cumplir con el estándar PCI es muy alta, pues según estadísticas las compañías que siguen esta regulación fortalecen los sistemas de seguridad y son poco vulnerables a los ataques cibernéticos alcanzado niveles de efectividad muy importantes[3].

No obstante, es de resaltar que en el proceso de activación de los servicios del cajero automático, ejecutan procedimientos inseguros que no prestan la fiabilidad a los usuarios que los utilizan; teniendo en cuenta que, el cargue de las llaves de cifrado es ejecutado de forma manual por dos (02) personas o custodios (ingeniero de campo asignado por la marca del cajero y el subgerente de la oficina) los cuales van a tener acceso a toda la información almacenada en el disco duro del cajero, lo que conlleva a fraudes, robos, clonación tarjetas, entre otros.

En referencia a lo anterior y con el objeto de garantizar cada uno de las propiedades de la información, se ve la necesidad de hacer el siguiente cuestionamiento:

¿Cómo las entidades del Sector Financiero Colombiano pueden reestructurar el procedimiento actual de generación de llaves de cifrado para cajeros electrónicos

[3] PÉREZ ARBESÚ, Lizzette Beatriz. Hallazgos sobre un estudio de PCI y protección de datos. Computerworld. México D.F. Editor at Ediworld SA de C.V. Octubre 26 de 2012. Disponible en Internet: http://www.computerworldmexico.mx/Articulos/25950.htm?goback=.gde_128300_member_179337052#

de forma automática sin la necesidad de que terceros puedan manipular la información contenida en el mismo?

## 1.3 OBJETIVOS

### 1.3.1 Objetivo General

Reestructurar el procedimiento de la generación de llaves de cifrado para cajeros electrónicos en el sector financiero Colombiano, para contribuir con la integridad y disponibilidad de la información almacenada en el disco duro de la máquina.

### 1.3.2 Objetivos Específicos

- ✓ Revisar el procedimiento actual de generación de llaves de cifrado para la activación de servicios de los cajeros electrónicos.
- ✓ Plantear alternativas hardware que provean las llaves de cifrado para que activen los servicios del cajero electrónico de forma automática y seleccionar la mejor.
- ✓ Reestructurar el procedimiento actual por un procedimiento de generación de llaves de cifrado de manera remota.

## 1.4 JUSTIFICACIÓN

La sustitución del billete en los bancos a nivel mundial, por el dinero plástico, es cada vez más frecuente; en Estados Unidos donde nació por impulso de las multinacionales, es habitual utilizarlo en lugares como: gasolineras, moteles, supermercados, centros comerciales, parques de diversiones, hoteles, etc., donde por razones de seguridad y control, se advierte que los pagos se deben efectuar únicamente con tarjetas de crédito o débito. La razón no es sólo, por la seguridad que supone, el que no haya dinero en billetes de banco en las cajas, es también porque la tarjeta con sus números de identificación, permite realizar estudios de mercado y de fidelidad de los clientes a un centro comercial o una cadena de hoteles[4].

[4] TRIGO CHACÓN, Manuel. Multinacionales, globalización y terrorismo. Madrid (España) Editorial Visión Libros, 2004. pág 216.

Por lo anterior, y teniendo en cuenta el avance tecnológico y el cambio constante en las organizaciones bancarias ante la fuerte competencia; las ha llevado que día a día aumenten la calidad de sus servicios para satisfacer las necesidades de sus clientes y eleven el crecimiento en el mercado competitivo, lo que conlleva, a implementar servicios online a través de internet, cajeros electrónicos, puntos de pago, entre otros; con estos servicios nace una nueva cultura, donde ya los soportes físicos de las transacciones desaparecen por completo dando origen a documentos digitales reduciendo las largas colas y la utilización de papel; pero a su vez está aumentando el delito electrónico, donde este tipo de información es frágil a ser capturada, manipulada y utilizada para fines personales por terceros.

Es por esto, que con la reestructuración de ingreso de llaves de forma automática se buscará que terceros no tengan acceso a la información interna del sistema, que se encuentra alojada en la computadora del cajero. Además se estará evitando un desgaste logístico como es el proceso de generar las componentes de cifrado de forma manual; para lo cual, el sistema lo realizará de manera automática con solamente ingresar al sistema operativo del cajero y dar un click al icono de carga remota de llaves. Todo este proceso hace parte garantizar la confiabilidad para los clientes finales y que las transacciones realizadas en este tipo de servicios queden almacenadas de forma segura; y no puedan ser accedidos y descifrados por terceros que tengan las llaves maestras de los cajeros automáticos.

## 1.5 ALCANCE Y LIMITACIONES

### 1.5.1 Alcance

Este proyecto está ubicado en la línea de criptografía y modelos formales, y busca proponer el procedimiento para la generación de llaves de cifrado de forma automática mediante una alternativa hardware que provee los dos (02) componentes de cifrado para la activación de los servicios de los cajeros automáticos.

### 1.5.2 Limitaciones

Es de resaltar que el desarrollo del presente proyecto, no enmarca temas como los que se definen a continuación:

- ✓ El procedimiento para la carga automática de llaves de cifrado será propuesto y no implementado.

- ✓ Si la reestructuración es aplicada en una entidad bancaria esta debe asumir los costos que conlleve el proceso.

- ✓ Quienes utilicen el proyecto deberán firmar acuerdo de confidencialidad con los autores.

## 1.6 DISEÑO METODOLÓGICO

Este proyecto se enmarca dentro de la definición metodológica de un enfoque descriptivo, explicativo y proyectivo.

### 1.6.1 Descriptivo

Tiene como objetivo central, lograr la descripción o caracterización de un evento de estudio dentro de un contexto particular. Consiste en identificar las características del evento estudiado.

### 1.6.2 Explorativo

Tiene como objetivo básicamente aproximarse a un evento poco conocido para familiarizarse con el, abriendo camino hacia otro tipo de investigación más compleja.

### 1.6.3 Proyectivo

También conocido como “proyecto factible”, consiste en la elaboración de una propuesta o modelo para solucionar determinadas situaciones. Se ubican las investigaciones para el diseño de programas de intervención social, de maquinarias, de programas informáticos, de inventos.

# 2. PROCEDIMIENTO ACTUAL DE GENERACIÓN DE LLAVES DE CIFRADO PARA CAJEROS AUTOMÁTICOS

## 2.1 OBJETIVO

Establecer los nuevos procedimientos, avalados por las franquicias VISA y MASTER CARD, para el manejo operativo de las llaves de cifrado en los cajeros automáticos en Colombia, con el fin de cumplir con las normas de seguridad establecidas en las circulares externas 052 de 2007 y 022 de 2010 emitido por la Superintendencia Financiera de Colombia y la norma de seguridad de datos PCI versión 2 de Octubre de 2010 que exigen a todos los Bancos como emisor de tarjetas, garantizar la seguridad y confidencialidad del PIN en los cajeros automáticos.

## 2.2 DESARROLLO DEL PROCESO

La llave “A” es la clave de trabajo exclusiva del cajero automático que permite el funcionamiento del mismo, ofreciendo seguridad a las operaciones realizadas por las tarjetas habientes. Está compuesta por 2 componentes alfanuméricos que se generan automáticamente utilizando un proceso aleatorio mediante el dispositivo TKE, su ingreso en el cajero automático es manual y su función es la de generar las otras llaves de seguridad del cajero automático.

### 2.2.1. Solicitud de la llave “A”

El Subgerente Operativo de la oficina es el responsable de solicitar la llave “A”, mediante un correo electrónico dirigido al área de seguridad de la información del Banco.

Esta petición es atendida por la dependencia de Seguridad de la información quien debe dar respuesta en el momento que sean enviados los dos nuevos componentes hacia la oficina solicitante.

Los eventos en los cuales debe solicitarse una nueva llave para cambiar la vigente en los cajeros automáticos son:

- Instalación del cajero automático por primera vez.
- Sospecha de conocimiento de la llave por personas no autorizadas.
- Desmonte o reubicación del cajero automático.

- Retiro del Banco de los dos (2) funcionarios que están asignados como custodios.

### 2.2.2 Generación de los componentes

Los funcionarios designados por las dependencias de Operaciones y Seguridad de la información son los responsables de la generación de los componentes de la llave “A”.

Éstos deben ser citados por Seguridad de la información cada vez que se requiera generar nuevos componentes para los cajeros automáticos actuales o nuevos. Para realizar la generación de los componentes de la llave “A”, Seguridad de la información debe solicitar el acceso físico al Site en donde se encuentra la consola TKE con previa antelación y los funcionarios asignados para la generación deben seguir con la procedimiento actual para la generación de los componentes.

### 2.2.3. Impresión de componentes de cifrado

Luego de haber realizado el procedimiento de generación de los dos componentes de cifrado se debe realizar la impresión en sobreflex; para ser enviados hacia la oficina solicitante.

### 2.2.4. Vulnerabilidades desarrollo del proceso

En el desarrollo del proceso de la generación de las llaves de cifrado se encontraron las siguientes vulnerabilidades ver tabla 1.

## 2.3. CONTROL COMPONENTES GENERADOS

Al culminar cada sesión, Seguridad de la información, debe realizar un acta con la descripción del proceso realizado, indicando la cantidad de componentes generados y entregados a correspondencia por parte del custodio respectivo, posteriormente todos los participantes revisaran y firmaran el acta.

### 2.3.1. Envío a la oficina de los componentes

Los funcionarios designados por las dependencias de Operaciones y Seguridad de la información, posterior a generar los componentes de las llaves de cifrado, son los responsables de enviarlos a las oficinas.

**Tabla 1:** Vulnerabilidades desarrollo del proceso

| GRUPO | DESCRIPCIÓN | VULNERABILIDAD |
|---|---|---|
| **Documentos/Datos** | Envió de Información sin protección | El envío de la solicitud de las llaves del cajero se realiza a través del correo electrónico institucional, sin utilizar un sistema de correo seguro, esto permite que terceros puedan leer la información. |
| **Software** | Administración deficiente de contraseñas | El control de acceso a la consola TKE es administrada por dos (02) funcionarios de las áreas comprometidas a quienes se les asigna las claves de acceso cada mes. Si los funcionarios seleccionados no se encuentran en el área; la misma clave debe ser entregada a su reemplazo. |
| **Personal** | Control inadecuado de reclutamiento | La generación de llaves de cifrado para los cajeros automáticos es contrato por el Banco con un tercero. |
| **Documentos/Datos** | Almacenamiento de datos no protegido | El borrado de memoria de la impresoras se debe hacer de forma manual después de haber impreso los componentes dos (02) de las llaves de cifrado. |
| **Documentos/Datos** | Solo copia | Los funcionarios encargados de realizar la impresión de los componentes (02) de las llaves de cifrados pueden duplicar la información |
| **Medio Ambiente e Infraestructura** | Protección Física Inadecuada – Sala | El área donde se encuentra la consola TKE no cuenta con una seguridad adecuada; donde se permite el ingreso de elementos como son: celulares, memorias USB, cables, y otros medios de comunicación que permiten el copiado de la información. |
| **Personal** | Definición de Rol Inadecuada | Los funcionarios para la generación de las llaves de cifrado para los cajeros son seleccionados al azar de las áreas involucradas; sin tener alguna responsabilidad sobre esta actividad. |
| **General** | Protección de Datos | Las llaves de cifrado generadas no tienen una seguridad adecuada y puede ser copiada o memorizadas por los funcionarios designados. |

Fuente: Propiedad de los autores

Para realizar el envío, deben guardar los componentes en sobres marcados y sellados, posterior, deben remitirlos a las oficinas respectivas a través de las empresas de correspondencia seleccionadas de la siguiente forma:

Primer día: El custodio 1 posterior a la generación y alistamiento de los sobres, debe realizar entrega de la parte 1 de cada llave generada al encargado de la correspondencia para su envío a las oficinas.

Tercer día: El custodio 2 posterior a la generación y alistamiento de los sobres, debe realizar entrega de la parte 2 de cada llave generada al encargado de la correspondencia para su envío a las oficinas.

La marcación de los sobres se realiza de la siguiente forma:

- No. Sobre
- Oficina (Nombre y Código)
- No. De cajero asignado
- No. Componente (1 o 2)
- Detalle: Principal o respaldo

### 2.3.2. Recepción en oficina de los componentes

El Subgerente Operativo de la oficina, es el responsable de recibir los sobres a la empresa de correspondencia, para lo cual debe firmar acuse de recibo.

Para dar conformidad en la recepción de los mismos, el subgerente debe enviar un correo electrónico a Seguridad de la información, en el que debe informar el nombre y código de los funcionarios asignados como responsables de los componentes recibidos.

Los acuses de recibo deben ser entregados por la empresa de correspondencia al área de Seguridad de la información en medio magnética, de tal forma que se pueda llevar control de los soportes de entrega.

Los sobres que contienen los componentes, que lleguen abiertos a las oficinas, con enmendaduras o cualquier otra señal de adulteración, deben ser devueltos en un sobre al área de Seguridad y solicitar inmediatamente la reposición del mismo utilizando el procedimiento establecido.

### 2.3.3. Custodia en oficina de los componentes

El Subgerente de la oficina, es el responsable de guardar SIN EXCEPCIÓN, en la caja fuerte y en sobre sellado, los componentes recibidos, por lo cual deberá utilizar cofres separados a su cargo, de tal forma que sea fácil la búsqueda en caso de ser solicitados nuevamente. En los casos que aplique, los sobres que contienen los componentes de respaldo deben ser guardados por el mismo responsable de la misma forma.

En todo momento los sobres deben permanecer sellados en el cofre de seguridad asignado; en caso de requerir la utilización de este, el custodio debe validar la integridad del sellado a fin de determinar que este no ha sido manipulado o abierto. En caso de evidenciar que el sobre ha sido abierto, se debe informar de inmediato al área de Seguridad de la Información para ejecutar el procedimiento de cambio de llaves de cifrado descrito en esta misma norma.

Los componentes de respaldo son generados para que la oficina cuente con llaves de cifrado como repuestos en los siguientes casos:

- Problemas al cargar componentes originales en el cajero.
- Perdida de componentes originales.
- Sospecha de conocimiento de la llave de cifrado por personas no autorizadas.
- Retiro del Banco de los dos (2) funcionarios que el Banco asignó como custodios

Cuando por alguna de las anteriores razones sea necesario utilizar los componentes de respaldo, es responsabilidad del Subgerente informar al área de Seguridad de la información y solicitar nuevos componentes para reemplazar los usados.

- Los sobres deben ser custodiados en las mismas condiciones que los componentes principales.
- En todo caso cada oficina debe contar con mínimo un componente de respaldo por cajero automático.

### 2.3.4. Vulnerabilidades control de componentes generados

En el desarrollo del control de los componentes de cifrados generados de las llaves de cifrado se encontraron las siguientes vulnerabilidades ver tabla 2.

## 2.4. INGRESO DE LA LLAVE “A” EN LOS CAJEROS AUTOMÁTICOS

El subgerente es el responsable del ingreso de los componentes en el cajero automático con ayuda del Ingeniero que da el soporte técnico a los cajeros automáticos.

Los eventos en los cuales debe ingresarse la llave en los cajeros automáticos son:

- Instalación del cajero automático por primera vez.
- Reinstalación de software.
- Actualización de llave por disposiciones de auditoría o de la franquicia.
- Cambio método de cifrado.
- Pérdida de la llave de cifrado por un golpe en el teclado del cajero.
- Sospecha de compromiso de la llave de cifrado

**Tabla 2:** Vulnerabilidades control de componentes generados

| GRUPO | DESCRIPCIÓN | VULNERABILIDAD |
|---|---|---|
| **Personal** | Definición del Rol Inadecuada<br>Falta de conciencia de Seguridad | Los funcionarios designados para la generación de los componentes; son los encargados de enviar a través de correspondencia certificada los sobres a la oficina solicitante; por lo anterior, los funcionarios tienen pleno conocimiento a que cajero se le ingresarán las llaves. |
| **Documentos/Datos** | Almacenamientos de documentos no estructurado | El sobre donde se almacena cada uno de los componente de las llaves de cifrado no son seguros; debido a que la forma de sellado se hace con pegamento de oficina para ser enviados a través de correspondencia certificada. |
| **Personal** | Falta de conciencia de seguridad | En primera instancia los sobres que contienen las llaves de cifrado estarán a cargo del subgerente de la oficina solicitante; quien puede tener previo conocimiento de las llaves de cifrado antes de ser designadas sus custodios. |
| **Documentos/Datos** | Solo Copia | Los custodios pueden realizar copiado de las llaves de cifrado; mediante técnicas de fotografía, escaneo, fotocopiado, microfilmación, etc. |
| **Documentos/Datos** | Envió de Información sin protección | El envío de la información del cajero automático se realiza a través del correo electrónico institucional, sin utilizar un sistema de correo seguro, esto permite que terceros puedan leer la información. |
| **General** | Protección de datos | Los dos (02) componentes de cifrados son almacenados en la misma bóveda de seguridad. Esto hace que la persona que tenga acceso al cofre pueda obtener la información completa de las llaves del cajero. |

Fuente: Propiedad de los autores

### 2.4.1. Vulnerabilidades ingreso de llaves en los cajeros automáticos

En el desarrollo del ingreso de la llave A en los cajeros automáticos se encontraron las siguientes vulnerabilidades ver tabla 3.

## 2.5. BITÁCORA LLAVE “A”

El Subgerente Operativo, es el responsable de llevar al día la bitácora de la llave “A” de cada uno de los cajeros automáticos de la oficina. La bitácora llave “A” es una herramienta que sirve para llevar el control de todos los eventos relacionados con la llave “A” del cajero automático. Este control debe ser por escrito en cuaderno o en medio magnético en un archivo de Hoja de Cálculo.

En esta bitácora llave “A” se debe registrar la siguiente información:

**Tabla 3:** Vulnerabilidades ingreso de llaves en los cajeros automáticos

| GRUPO | DESCRIPCIÓN | VULNERABILIDAD |
|---|---|---|
| **Personal** | Definición del Rol Inadecuada<br>Falta de conciencia de Seguridad | El ingreso de las llaves de cifrado de los cajeros automáticos está a cargo del ingeniero de campo asignado por la marca del cajero y el subgerente de la oficina quienes pueden vulnerar los datos de la computadora del cajero y obtener la información sensible del mismo. |
| **Documentos/Datos** | Almacenamiento de datos no Protegido | Luego de realizar el ingreso de la llave de cifrado al cajero, los dos (02) componentes quedan abiertos y en custodia de una sola persona (subgerente de la oficina) quien puede realizar copias de los datos alfanuméricos. |
| **Personal** | Falta de políticas/normas y procedimientos | Al ingresar las llaves de cifrado a los cajeros para la habilitación de los servicios; el sistema no bloquearan automáticamente los componentes; esto hace que estas llaves puedan ser copias y utilizadas en otros cajeros. |

Fuente: Propiedad de los autores

- Motivo: Ingreso - Destrucción.
- Fecha.
- No. Sobre.
- Tipo de Componente (1 ó 2)
- Número del cajero.
- Nombre de cada uno de los responsables del ingreso de las llaves de cifrado o de los suplentes que intervienen.
- Firmas.

### 2.5.1. Vulnerabilidades bitácora de las llaves cifrado

En el desarrollo del control que se debe llevar en la bitácora de las llaves de cifrado se encontraron las siguientes vulnerabilidades tabla 4.

**Tabla 4**: Vulnerabilidad bitácora de las llaves cifrado

| GRUPO | DESCRIPCIÓN | VULNERABILIDAD |
|---|---|---|
| **Documentos/Datos** | Almacenamiento de datos no Protegido | La información de la llave A del cajero queda en conocimiento de una sola persona quien es el Subgerente de la oficina. |
| **Software**<br>**Documentos/Datos** | Administración deficiente de contraseñas<br>Almacenamiento de datos no Protegido | Los datos del ingreso de las llaves de cifrado del cajero quedan guardados en un cuadro de mando en Excel sin medidas de seguridad. |
| **Documentos/Datos** | Inadecuada Protección de Activos | El acta de ingreso de los componentes de cifrado del cajero queda guardada en una carpeta A-Z y en un armario de la oficina a la vista de los todos funcionarios. |

Fuente: Propiedad de los autores

## 2.6. ACTIVACIÓN DE LA LLAVE “A” EN HOST

Para realizar la activación de la llave “A” en el cajero automático, el subgerente debe realizar una llamada al Centro de Gestión de Red (CGR) para informar que las llaves de cifrado fueron ingresadas al cajero, posterior a esto el CGR realiza la activación en el Host.

## 2.7. DESTRUCCIÓN DE LA LLAVE “A”

El Subgerente Operativo, es el responsable del proceso de destrucción la llave “A” de los cajeros automáticos.

Los eventos en los cuales debe destruir la llave en los cajeros automáticos son:

- Sospecha de conocimiento de la llave por personas no autorizadas.
- Desmonte o reubicación del cajero automático.
- Cuando se realice la solicitud de una nueva llave de cifrado.

Para realizar la destrucción de la llave “A”, el Subgerente Operativo, debe solicitar al área de Seguridad de la Información que asignen, previo conocimiento suyo, el funcionario que estará a cargo de la destrucción material de los sobres que contienen los componentes de las llaves de cifrado. Una vez asignado el funcionario, el subgerente debe entregar los sobres para que se realice la incineración de los mismos.

Al finalizar la destrucción de los sobres, el Subgerente de la oficina debe levantar un acta y hacerla firmar por los que intervinieron.

### 2.7.1. Vulnerabilidades de la destrucción de las llaves

En la destrucción de las llaves de cifrado se encontraron las siguientes vulnerabilidades que se resumen en la tabla 5.

Tabla 5: Vulnerabilidades de la destrucción de las llaves

| GRUPO | DESCRIPCIÓN | VULNERABILIDAD |
|---|---|---|
| **Personal General** | Falta de conciencia de Seguridad Protección de Datos | La destrucción de los componentes de cifrado se llevara a cabo por dos personas (subgerente de la oficina y funcionario designado por el área de operaciones) quienes son los encargados de la destrucción de los sobres. Quienes a su vez pueden obtener la información contenida en los mismo a través de copias. |
| **Documentos/Datos** | Inadecuada Protección de Activos | El acta de la destrucción de los sobres queda guardada en una carpeta A-Z y en un armario de la oficina a la vista de los todos funcionarios. |

Fuente: Propiedad de los autores

# 3. ALTERNATIVAS DE DISEÑO PARA EL NUEVO PROCEDIMIENTO DE GENERACIÓN DE LLAVES DE CIFRADO DE FORMA AUTOMÁTICA PARA CAJERO ELECTRÓNICOS

En la primera parte del proyecto se analizó el problema así como los objetivos a cumplir para dar mitigar las vulnerabilidades que tiene el procedimiento actual de generación de llaves de Cifrado. La sección que se describe a continuación se construye con el propósito de analizar las alternativas hardware existentes en el mercado que permia la reestructuración del procedimiento actual de generación de llaves de cifrado para cajeros electrónicos y que cumpla con los requerimientos establecidos por las normas de seguridad en sus circulares externas 052 de 2007 y 022 de 2010 emitido por la Superintendencia Financiera de Colombia y la norma de seguridad de datos PCI versión 2 de Octubre de 2010.

A continuación se describe las alternativas hardware para la restructuración del procedimiento actual

## 3.1. ALTERNATIVAS DE DISEÑO

El objetivo de esta etapa es establecer las posibles alternativas de solución. Se identifican las descripciones técnicas, operativas y financieras de acuerdo a cada una y se establece la viabilidad y alcance del proyecto.

Para llevar a cabo la realización del proyecto se tendrán en cuenta las siguientes alternativas.

### 3.1.1 Primera Alternativa - Futurex Series RKMS[5]

Este dispositivo es un servidor que administra claves y su interacción es directamente con el Host o en el procesamiento de transacciones y de forma remota distribuye las llaves de cifrado directamente a los cajeros automáticos. El proceso de la transferencia de llaves es rápido, el costo se reduce y se aumenta la seguridad entre los componentes de claves que ya no va ser necesario el ingreso manualmente en el cajero.

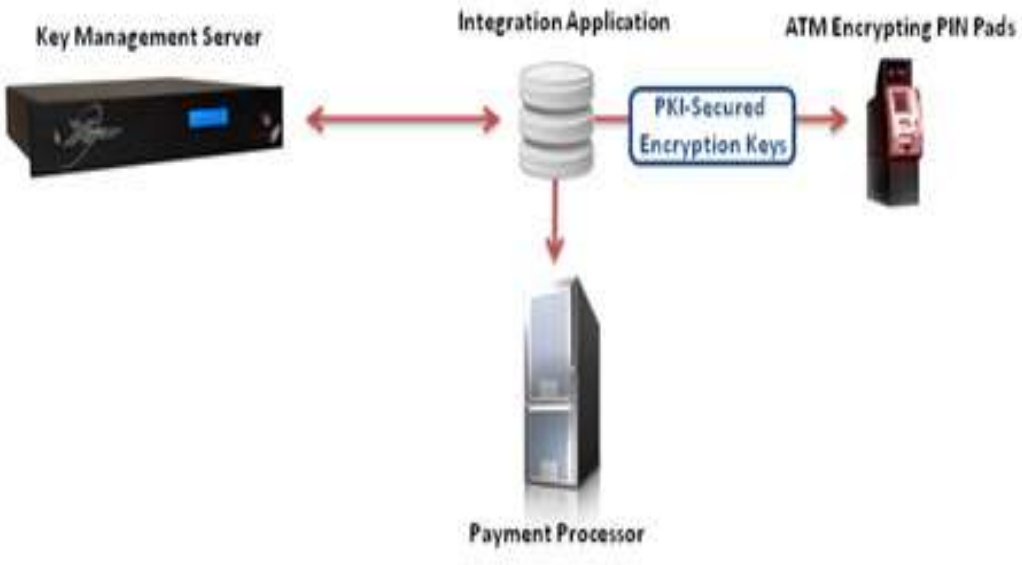
[5] FUTUREX COMPANY. Certificate Authority Server. Estados Unidos, Enero 2011. Disponible en Internet: http://www.futurex.com/products_general_caserver.asp

La serie RKMS ofrece una amplia gama de funciones de gestión de claves de cifrado, incluyendo la generación de claves, la distribución, la inyección, la eliminación y el seguimiento. También segura y remota distribuye las claves de cifrado sobre una red IP segura, eliminando de esta manera el proceso manual y engorroso de tener que físicamente ingresar las claves del cajero.

### 3.1.1.1 Diseño Funcional

Con el fin de ser automatizado, el proceso de distribución de claves se debe realizar en un entorno de acogida impulsado en la que el host actúa como un procesador intermedio entre el ATM y el servidor de gestión de claves. El anfitrión, a través de una aplicación de integración, solicitará la información requerida de ambos dispositivos y facilitará la transmisión de datos entre los dos. La integración de aplicaciones se puede ejecutar en el marco del programa de acogida o en un servidor dedicado, figura 1.

**Figura 1:** Modelo de funcional del Futurex Series RKMS




Fuente: Futurex Series RKMS - Establishing a Secure, Convenient, and Cost-Effective Remote Key Loading Environment. Disponible en Internet: http://www.futurex.com/blog/?p=78

Este servidor ofrece características innovadoras para la automatización del proceso a distancia manual de reemplazo de claves de cifrado. Después de cambiar la clave maestra del cajero, los agentes clave de seguridad, de forma remota pueden actualizar la Serie RKMS simplemente usando una web segura y/o e-mail interfaz.

### 3.1.1.2 Diseño Técnico

**a. Requerimientos Software**

- **Requerimientos Software de la Plataforma Servidor**

  No existen requerimientos software

- **Requerimientos Software Plataforma Autoservicio**

  Microsoft Windows XP

**b. Requerimientos Hardware**

- **Plataforma Servidor**

  No existen requerimientos hardware

**c. Condiciones de funcionamiento**

Requisitos de energía: 100 - 230 VAC 50/60 Hz. 400 Watts
Temperatura de funcionamiento: 50 ° a 95 ° F (10 ° a 35 ° C)
Temperatura de almacenamiento: -40 ° a 149 ° F (-40 ° a 65 ° C)
Humedad relativa: 20% a 80% sin condensación
Humedad relativa de almacenamiento: 5% a 95% sin condensación

**d. Cumple con los estándares de la industria de cumplimiento**

PCI DSS
FIPS 140-2 Nivel 3-compatible
ANSI X9.24 parte 1 y parte 2 para la administración de claves simétricas y asimétricas - TR-39

**e. Certificaciones**

No tiene certificaciones asociadas

**f. Conjunto de aplicaciones Futurex Series RKMS**

No relaciona aplicaciones adicionales

### 3.1.1.3 Diseño Económico

El costo de adquirir el Futurex Series RKMS se presenta en la tabla 6.

**Tabla 6**: Costo de adquisición del Futurex Series RKMS

| DESCRIPCIÓN | CANTIDAD | USD |
|---|---|---|
| **Futurex Series RKMS** | 1 | 92.400 |
| **Mantenimiento** | 1 | 13.860 |

Fuente: Propia de los autores

### 3.1.1.4 Características

- Automatiza el proceso manual de reemplazo clave.
- Inyecta las claves de cifrado a través de una conexión TCP/IP.
- Administrar claves desde una ubicación central.
- Alta Seguridad y protección de Claves: TAMPER RESISTANT.
- Genera e imprimir los componentes de clave de forma manual.
- Integrado, basado en hardware de recuperación de desastres y redundancia.
- Soporta DES y 3DES.
- Robusto, basado en permisos de usuario del sistema de gestión para la separación de funciones.
- Batería de respaldo para las llaves en la memoria TRSM.
- Multiusuario de agrupación de restricción de acceso.
- Software cliente Multi-vendor: DIEBOLD, NCR.

### 3.1.1.5 Ventajas

- Elimina el costo del proceso manual de carga llaves.
- Remota y simplemente actualiza sus unidades mediante el uso de una web segura y / o e-mail interfaz.
- Ayuda a reducir los costos de administrativa y formación.
- Automatización del proceso manual de reemplazo de claves.
- Proporciona autenticación dual.
- Instantánea y completa los registros de auditoría para todas sus claves actualizadas.
- Automatiza los procesos clave manual y remoto de reemplazo en un grado definido por el fabricante.
- Forma remota y segura inyecta claves de cifrado en los dispositivos en el punto de fabricación.
- Después de cambiar la clave maestra de archivos, los agentes clave de forma remota puede actualizar la Serie RKMS simplemente usando un web seguro y / o e-mail interfaz.
- Acceso administrativo vía web.
- Se ajusta al hardware existente.

### 3.1.1.6 Desventajas

- Funciona únicamente con cajeros marca DIEBOLD y NCR.
- No funciona con el protocolo de comunicaciones SNA.
- No tiene modulo de seguridad de hardware HSM.
- El dispositivo no genera las llaves iniciales de cifrado de forma automática.
- Se deben adquirir las llaves de cifrado por separado para ser administradas por el dispositivo.
- La protección de la clave inicial únicamente lo hace con TAMPER RESISTANT.
- Los reportes de generación de llaves de cifrado se deben hacer de forma manual.
- Las llaves deben ser ingresadas de forma manual para su administración.
- El mantenimiento de los equipos lo hace el proveedor de la marca y no el banco.

## 3.1.2 Segunda Alternativa Cryptosec-RKL[6]

Criptosec-RKL, es una solución integrada de RKL (Remote Key Loading) o carga remota de claves para cajeros, TPV's y PinPad; Criptosec-RKL es un servidor de carga remota de claves "Multi-vendor", que implementa los esquemas de carga de los principales fabricantes de cajeros automáticos: Diebold, NCR, Wincorn, Fujitsu entre otros.

Uno de los principales objetivos de la solución es que ésta no requiera cambios hardware y software en el Host a la hora de integrar el dispositivo con la parte operativa funcional , y además no plantea la necesidad de cambios en la Aplicación que se ejecuta actualmente en los Autoservicios. Se trata por tanto de lograr que la solución tenga una autonomía completa y no requiera integración con los sistemas Host.

### 3.1.2.1 Diseño Funcional

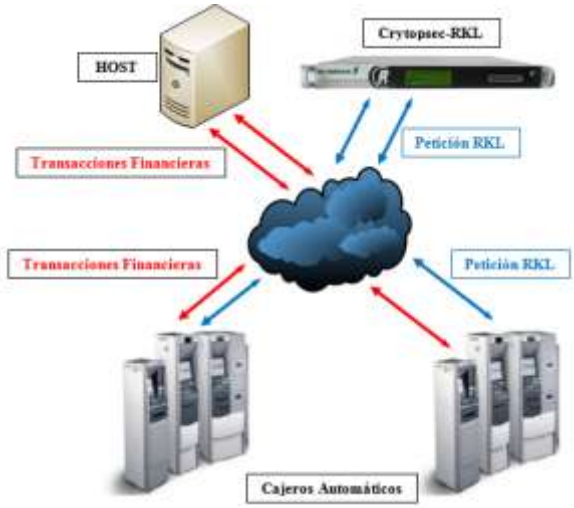
La solución Cryptosec-RKL utiliza un módulo de seguridad tamper-resistant y tamper-responsive, en cuya memoria residirían las Claves Master de Transporte para las distintas marcas de cajeros automáticos adheridos al servicio de RKL.

[6] IGVANOVA, Velianna, RODRIGUEZ CABRERO, Jesús y GORDO, José Alberto. Visión de conjunto y características técnicas de Cryptosec-RKL. Madrid. Editado por Realsec. Febrero 2010. Disponible en Internet: http://www.realsec.com/pdfProEs/Cryptosec-RKL.pdf

El servidor recibirá peticiones procedentes de los ATM para la carga de la clave inicial de los diferentes cajeros. Finalizada la sesión de transmisión de la clave inicial para el Autoservicio en cuestión, éste estará en condiciones para iniciar operaciones contra el Host de la manera habitual sin necesidad de dialogar nunca más con el Servidor Cryptosec-RKL. En estos dos últimos supuestos, el proceso de petición de carga de claves será lanzado de nuevo por la aplicación de Autoservicio, de forma automática y transparentemente para el personal técnico o de la oficina.

Una vez completado el proceso de carga de la Clave inicial por cada cajero inicializado, la aplicación de Autoservicio comunicaría la nueva condición del cajero como “inicializado” a la Solución de Gestión de Red como se muestra en la figura 2.

**Figura 2:** Modelo de funcional del Cryptosec-RKL




Fuente: Realsec - Visión de conjunto y características técnicas de Cryptosec-RKL. Disponible en Internet: http://styt.co/wp-content/uploads/2011/03/Cryptosec-RKL.pdf

### 3.1.2.2 Diseño Técnico

### a. Requerimientos Software

- **Requerimientos Software de la Plataforma Servidor**

  No existen requerimientos software

- **Requerimientos Software Plataforma Autoservicio**

  Microsoft Windows XP

**b. Requerimientos Hardware**

- **Plataforma Servidor**

  No existen requerimientos hardware

- **Modulo de Seguridad HSM**

  El sistema incorpora el HSM **CryptoSec 2048** de REALSEC. El modelo HSM cubre el conjunto de primitivas criptográficas necesarias para la gestión de generación y verificación de firmas utilizando algoritmos asimétricos. La consola de seguridad ofrece extensas posibilidades de gestión de las claves que residen en el sistema y de la administración de la los usuarios con derechos de acceso al sistema, de los custodios de la Clave Master del equipo y la programación de las operaciones de mantenimiento entre otros.

**c. Condiciones de funcionamiento**

Requisitos de energía: 100 - 240 V AC, 47/63 Hz. 100 Watts
Temperatura Operacional. 10 ° C to 40 ° C sin condensación.
Humedad: 10% - 90%

**d. Cumple con los estándares de la industria de cumplimiento**

EPP XFS 3.0
ANIS X9.24-1
FIPS 140-2 Level 3 and Common Criteria EAL4+, covering the Hardware Security Module
PCI DSS

**e. Certificaciones**

FIPS 140-2, level3 y Common Criteria EAL 4+

**f. Conjunto de aplicaciones Cryptosec–RKL**

La solución cuenta los siguientes módulos software:

**RtCore**– este componente recibe y procesa las peticiones de carga remota de claves que recibe procedentes del parque de Cajeros. Se responsabiliza de la programación de las primitivas criptográficas del modulo de seguridad, para brindar la funcionalidad requerida según el esquema especifico RKL.

**RtInterfaces**– Cryptosec-RKL se comunica con entidades externas tales como los cajeros a través de interfaces. Las interfaces llevan a cabo las comunicaciones entre el sistema Cryptosec- RKL y el mundo exterior. Son los responsables de ejecutar el protocolo de carga de claves específico para cada uno de los fabricantes, llevando primero la Autenticación Bilateral y posteriormente utilizando el canal seguro establecido transmiten la clave Inicial del Autoservicio. Todos los mensajes enviados entre el **RtCore** y los **RtInterfaces**, son formateados de acuerdo con protocolo especifico por cada fabricante, usando como protocolo de comunicaciones el estándar TCP/IP.

**RtOffice** – es el componente encargado de los procesos de gestión de las bases de Datos, el manejo de los datos necesario para el correcto funcionamiento del sistema y de la generación de informes.

**RtAdmin –** Es el modulo de administración de la solución Cryptosec-RKL, que a través del GUI permite la configuración de la solución con los datos necesario para el optimo funcionamiento del sistema y su gestión administrativa.
**RtAgent –** se trata de un componente que reside en el cajero y que durante el arranque del autoservicio determinara la necesidad de iniciar el proceso de petición de la clave inicial a Cryptosec-RKL.

### 3.1.2.3 Diseño Económico

El costo de adquirir el Cryptosec-RKL se presenta en la siguiente tabla.

**Tabla 7**: Costo de adquisición del Cryptosec-RKL

| DESCRIPCIÓN | CANTIDAD | USD |
|---|---|---|
| **Cryptosec-RKL** | 1 | 81.600 |
| **Mantenimiento** | 1 | 12.240 |

Fuente: Propia de los autores

### 3.1.2.4 Características

- Servidor integrado: Hardware/software, Aplicación de carga remota y HSM.
- Arquitectura Cliente basada en estándar EPP XFS.
- Software cliente Multi-vendor: DIEBOLD, NCR, WINCOR, FIJITSU etc.
- Alta Seguridad y protección de Claves: TAMPER RESISTANT y RESPONSIVE.
- Sistema independiente del HOST y Autoservicios
- Protocolos de Comunicación estandares : TCP/IP, X.25 etc.
- Generación y verificación de Claves y Firmas en HSM ( certificado FIPS 140-2 Level 3)
- Sistema basado en normas ANSI y estándares VISA y MASTERCARD.

- Alta disponibilidad y aceleración criptográfica ( 2.400 t.p.s )
- Conforme a normas ANSI X 9.
- Frecuencia de distribución definible.

#### 3.1.2.5 Ventajas

- Fácil de administrar
- Arquitectura Cliente multivendor – NCR, WINCOR, DIEBOLD, FIJITSU, ITAUTEC etc.
- Arquitectura Cliente - basada en estándar XFS
- Arquitectura Servidor abierta - basada en la plataforma tecnológica .NET
- Independencia de los modelos actuales de los procesos operativos del Host y Autoservicios.
- Automatización del proceso manual del reemplazo de claves.
- Instalación automática y remota de las llaves.
- Seguridad entre el cliente-servidor en la autenticación de protocolo utilizando criptografía asimétrica.
- Sistema basado en normas ANSI y estándares VISA y MASTERCARD.
- Tiene certificaciones en FIPS 140-2, level3 y Common Criteria EAL 4+
- Compatible con los estándares tecnológicos de la industria (ANSI, PCI, etc.)
- Elimina el costo del proceso manual de cargas de llaves
- No requiere de hardware y software adicional.

#### 3.1.2.6 Desventajas

- No es administrable de forma remota a través de interfaz WEB segura.
- El dispositivo no genera las llaves iniciales de forma automática.
- Se deben adquirir las llaves de cifrado por separado para ser administradas por el dispositivo.
- El mantenimiento de los equipos lo hace el proveedor de la marca y no el banco.
- No tiene fuente redundante.

### 3.1.3 Tercera Alternativa – ProRKL Wincor Nixdorf[7]

Wincor Nixdorf presenta la solución integrada de ProRKL (Pro - Remote Key Loading) o Protocolo Dependiente de carga remota de claves para cajeros que permite introducir de forma remota las llaves a las terminales y subir el servicio de los cajeros automáticos sin necesidad de visitar el lugar.

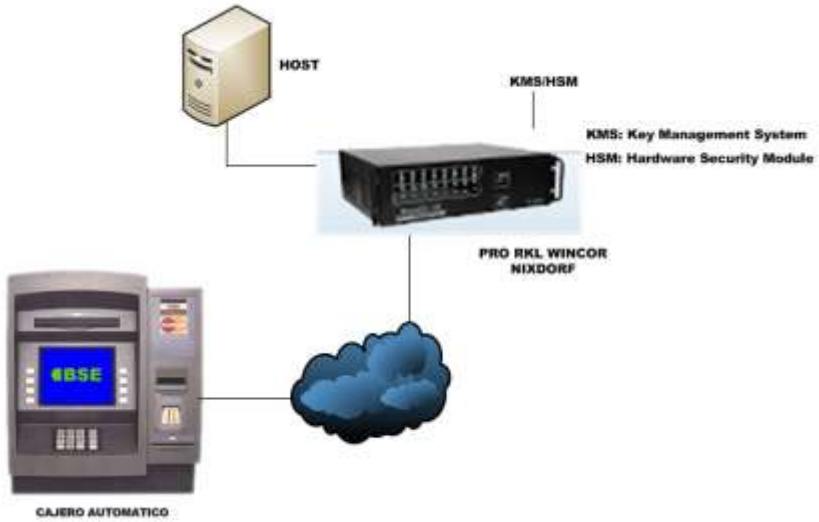
[7] WINCOR NIXDORF International GmbH. ProRKL Central master key distribution and loading in self – service nerworks. Germany. Printed in Germany, January 2006. Disponible en Internet: http://www.wincor-nixdorf.com/internet/site_ASP/ASP/Products/Software/Banking/SecurityProcess/RKL/RKL.html

### 3.1.3.1 Diseño Funcional

Con el fin de ser automatizado, el proceso de distribución de claves se debe realizar en un entorno de acogida impulsado en la que el host actúa como un procesador intermedio entre el ATM y el servidor de gestión de claves. El anfitrión, a través de una aplicación de integración, solicitará la información requerida de ambos dispositivos y facilitará la transmisión de datos entre los dos. La integración de aplicaciones se puede ejecutar en el marco del programa de acogida o en un servidor dedicado.

Consta de un Agente RKL, Server RKL y conectores para los diferentes RKL Switch / Host sistemas, Sistemas de gestión de claves y módulos de seguridad de hardware, PT / E-RKL, construido alrededor de una moderna arquitectura de varios niveles, ver figura 3.

**Figura 3:** Modelo funcional del ProRKL




Fuente: ProRKL (Pro - Remote Key Loading). Disponible en Internet: http://www.wincor-nixdorf.com/internet/cae/servlet/contentblob/186310/publicationFile/7771/Broschuere_RKL_EN.pdf

### 3.1.3.2 Diseño Técnico

#### a. Requerimientos Software

- **Requerimientos Software de la Plataforma Servidor**

  No existen requerimientos software
- **Requerimientos Software Plataforma Autoservicio**

  Microsoft Windows XP

**b. Requerimientos Hardware**

- **Plataforma Servidor**

  No existen requerimientos hardware

**c. Condiciones de funcionamiento**

No relaciona condiciones de funcionamiento

**d. Cumple con los estándares de la industria de cumplimiento**

PCI DSS
ANSI y estándares VISA y MASTERCARD.
FIPS 140-2, level3 y Common Criteria EAL 4+

**e. Certificaciones**

No relaciona certificaciones

**f. Conjunto de aplicaciones**

No relaciona aplicaciones

### 3.1.3.3 Diseño Económico

El costo de adquirir el ProRKL Wincor Nixdorf se presenta en la siguiente tabla.

**Tabla 8**: Costo de adquisición del ProRKL Wincor Nixdorf

| DESCRIPCIÓN | CANTIDAD | USD |
|---|---|---|
| **ProRKL Wincor Nixdorf** | 1 | 75.350 |
| **Mantenimiento** | 1 | 11.302 |

Fuente: Propia de los autores

### 3.1.3.4 Características

- Reducción de los costos de mantenimiento de cajeros automáticos y costos personales.
- Sistema de administración de claves.
- Es una solución Multivendor para las marcas Wincor e IBM.
- Mayor seguridad.
- Cumple con los requisitos de cartas diferentes (PCI, ANSI, FIPS 140-2).
- Protección de Claves: TAMPER RESPONSIVE.

- Soporta DES y 3DES.
- Soporta distribución de firmas.
- Protocolo de comunicación TCP/IP.
- Carga automática en todos los cajeros automáticos.
- Apoyo a ambas firmas y claves de certificados.
- Se utiliza como estándares abiertos por Wincor Nixdorf NDC / DDC extensiones de protocolo RKL.
- ProRKL le ofrece la RKL protocolo extensiones de Wincor Nixdorf, NCR e IBM.

#### 3.1.3.5 Ventajas

- Fácil de administrar.
- ProRKL le ofrece la RKL protocolo extensiones de Wincor Nixdorf, NCR, e IBM.
- Se utiliza como estándares abiertos por Wincor Nixdorf NDC / DDC extensiones de protocolo RKL.
- Elimina el costo del proceso manual de cargas de llaves.
- Es una solución Multivendor para marcas Wincor e IBM..
- No requiere de hardware y software adicional.

#### 3.1.3.6 Desventajas

- No es administrable de forma remota a través de interfaz WEB segura.
- Funciona únicamente para dos marcas de cajeros Wincor Nixdorf e IBM.
- No funciona con el protocolo de comunicaciones SNA.
- No tiene modulo de seguridad de hardware HSM.
- El dispositivo no genera las llaves iniciales de cifrado de forma automática.
- Se deben adquirir las llaves de cifrado por separado para ser administradas por el dispositivo.
- La protección de la clave inicial únicamente lo hace con TAMPER RESPONSIVE.
- Los reportes de generación de llaves de cifrado se deben hacer de forma manual.
- Las llaves deben ser ingresadas de forma manual para su administración.
- El mantenimiento de los equipos lo hace el proveedor de la marca y no el banco.

### 3.1.4 Cuarta Alternativa – EFTSec[8]

EFTSec elimina los riesgos de fraude en las redes transaccionales gracias a su avanzado sistema de encriptación punto a punto. Los datos del tarjetahabiente son

[8] PANDAID, Soluciones C.A. EFT Transaction Security (EFTSec) Conectividad. Venezuela, 2012. Disponible en Internet: http://www.pandaid.com/eftsec/

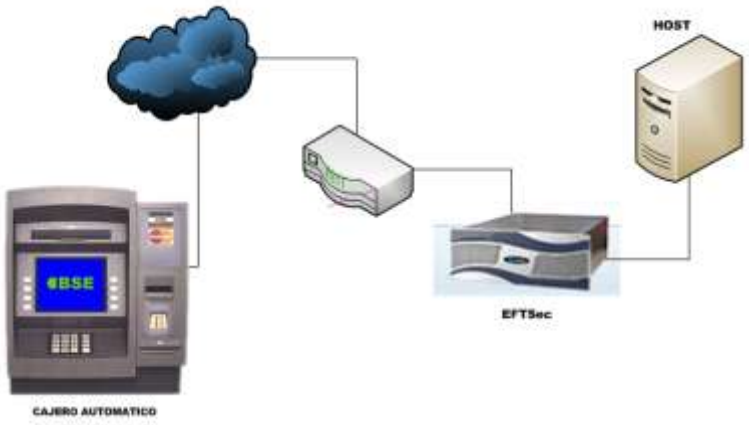
cifrados en el terminal de pago viajando de forma segura hasta un punto de confianza, donde son descifrados y procesados. EFTSec requiere un mínimo de gastos operativos y administrativos además de una sencilla instalación.

### 3.1.4.1 Diseño Funcional

EFTSec permite que una parte o todo el conjunto de datos de una transacción que pasa entre un cajero y una Red de Acceso sean cifrados, convirtiéndose en una información segura desde cualquier ataque comercialmente viable. Funciona como una extensión (Plug-In) Punto a Punto instalada en la red que no implica una perturbación en el tráfico de su infraestructura haciendo que la implementación sea transparente.

Es ideal para instituciones financieras y comerciales que requieren preservar su inversión actual y cumplir con las últimas normas que rige la ley en materia de comunicación de datos bancarios, además EFTSec cuenta con el respaldo de ser una solución probada con más de 3.4 millones de transacciones seguras por mes ejecutadas a nivel mundial.

**Figura 4**: Modelo de funcional del EFTSec




Fuente: EFT Transaction Security (EFTSec). Disponible en Internet: http://es.scribd.com/doc/45498516/EFT-Transaction-Security-April-2007

### 3.1.4.2 Diseño Técnico

#### a. Requerimientos Software

- **Requerimientos Software de la Plataforma Servidor**

  No existen requerimientos software

- **Requerimientos Software Plataforma Autoservicio**

  Microsoft Windows 2003/2008 o superior
  MS SQL 2005/2008 o superior

**b. Requerimientos Hardware**

- **Plataforma Servidor**

  No existen requerimientos hardware

**c. Condiciones de funcionamiento**

No registra condiciones de funcionamiento

**d. Cumple con los estándares de la industria de cumplimiento**

Manejo de llaves: DUKPT y llaves maestras o de sesión FIPS 140-2, Nivel 3 HSM validado

**e. Certificaciones**

No relaciona certificaciones

**f. Conjunto de aplicaciones EFTSec**

No relaciona aplicaciones

### 3.1.4.3 Diseño Económico

El costo de adquirir el EFTSec se presenta en la siguiente tabla.

**Tabla 9**: Costo de adquisición del EFTSec

| DESCRIPCIÓN | CANTIDAD | USD |
|---|---|---|
| **EFTSec** | 1 | 85.450 |
| **Mantenimiento** | 1 | 12.817 |

Fuente: Propia de los autores

### 3.1.4.4 Características

- Motor de cambio de transacciones de alto rendimiento.
- Capacidad de cifrar una porción del mensaje o su totalidad.
- Altamente escalable con reparto de carga distribuida.

- Soporta DES
- Utiliza el estándar de la industria HSM (Hardware Security Module) para el cifrado y descifrado de datos transaccionales que proveen
- Validación en entornos FIPS 140-2, Nivel 3
- Soporte de administración de llaves con el estándar HSM.
- Protocolo de comunicación TCP/IP y SNA.
- Soporte de distribución de llaves seguras vía Dial-Up, línea dedicada o Smart Card.

#### 3.1.4.5 Ventajas

- Fácil de administrar
- Capacidad de cifrar una porción del mensaje o su totalidad
- Utiliza el estándar de la industria HSM (Hardware Security Module) para el cifrado y descifrado de datos transaccionales que proveen validación en entornos FIPS 140-2, Nivel 3.
- Soporte de administración de llaves con el estándar HSM
- Elimina el costo del proceso manual de cargas de llaves
- Es una solución Multivendor.
- No requiere de hardware y software adicional.

#### 3.1.4.6 Desventajas

- Funciona únicamente con cajeros marca DIEBOLD y NCR.
- No funciona con el protocolo de comunicaciones SNA.
- No tiene modulo de seguridad de hardware HSM.
- El dispositivo no genera las llaves iniciales de cifrado de forma automática.
- Se deben adquirir las llaves de cifrado por separado para ser administradas por el dispositivo.
- La protección de la clave inicial únicamente lo hace con TAMPER RESISTANT.
- Los reportes de generación de llaves de cifrado se deben hacer de forma manual.
- Las llaves deben ser ingresadas de forma manual para su administración.
- El mantenimiento de los equipos lo hace el proveedor de la marca y no el banco.

## 3.2 COMPARACIÓN DE ALTERNATIVAS HARDWARE PARA LA GENERACIÓN REMOTA DE LLAVES DE CIFRADO

| ALTERNATIVAS | VENTAJAS | OBSERVACIONES |
|---|---|---|
| **Futurex Series RKMS** | • Elimina el costo del proceso manual de carga llaves.<br>• Por medio remoto y simplemente actualiza sus unidades mediante el uso de una web segura y / o e-mail interfaz.<br>• Ayuda a reducir los costos de administrativa y formación.<br>• Automatización del proceso manual de reemplazo de claves.<br>• Proporciona autenticación dual.<br>• Instantánea y completa los registros de auditoría para todas sus claves actualizadas.<br>• Automatiza los procesos clave manual y remoto de reemplazo en un grado definido por el fabricante.<br>• Forma remota y segura inyecta claves de cifrado en los dispositivos en el punto de fabricación. Acceso administrativo vía web.Se ajusta al hardware existente. | ✓ Multivendor en cajeros Diebold y NCR.<br>✓ Protocolo de comunicación TCP/IP.<br>✓ Seguridad para las Claves es por Tamper Resistant.<br>✓ Genera e imprime los componentes de claves de forma manual.<br>✓ Multiusuario de agrupación con restricción de acceso, solamente los permisos lo da el fabricante.<br>✓ Estandar PCI DSS, FIPS 140-2, ANSI X9.24.<br>✓ Costo y mantenimiento anual del dispositivo es USD 106.260 |
| **CRYPTOSEC – RKL** | • Fácil de administrar<br>• Arquitectura Cliente multivendor – NCR, WINCOR, DIEBOLD, FIJITSU, ITAUTEC etc.<br>• Arquitectura Cliente - basada en estándar XFS<br>• Arquitectura Servidor abierta - basada en la plataforma tecnológica .NET<br>• Independencia de los modelos actuales de los procesos operativos del Host y Autoservicios.<br>• Automatización del proceso manual del reemplazo de claves.<br>• Instalación automática y remota de las llaves.<br>• Seguridad entre el cliente-servidor en la autenticación de protocolo utilizando criptografía asimétrica. | ✓ Es Multivendor para cualquier marca de cajeros.<br>✓ Protocolo de comunicación TCP/IP, SNA y X.25.<br>✓ Estandar PCI DSS, FIPS 140-2, ANSI X9.24 y Visa y Mastercard.<br>✓ Presenta el módulo HSM para generación y certificación de claves.<br>Seguridad de las Claves es por Tamper Resistant y Responsive. |

| ALTERNATIVAS | VENTAJAS | OBSERVACIONES |
|---|---|---|
| **CRYPTOSEC – RKL** | • Sistema basado en normas ANSI y estándares VISA y MASTERCARD.<br>• Tiene certificaciones en FIPS 140-2, level3 y Common Criteria EAL 4+<br>• Compatible con los estándares tecnológicos de la industria (ANSI, PCI, etc.)<br>• Elimina el costo del proceso manual de cargas de llaves<br>• No requiere de hardware y software adicional. | ✓ Sistema independiente del HOST y Cajeros.<br>✓ Genera reportes de forma automática al administrador.<br>✓ Costo y mantenimiento anual del dispositivo es USD 93.840 |
| **PRO RKL WINCOR NIXDORF** | • Fácil de administrar<br>• ProRKL le ofrece la RKL protocolo extensiones de Wincor Nixdorf, NCR, Diebold NDC y DDC<br>• Se utiliza como estándares abiertos por Wincor Nixdorf NDC / DDC extensiones de protocolo RKL<br>• Elimina el costo del proceso manual de cargas de llaves<br>• Es una soluciones Multivendor<br>• No requiere de hardware y software adicional. | ✓ Solución Multivendor para las marcas Wincor, IBM y NCR.<br>✓ Protocolo de comunicación TCP/IP.<br>✓ Estandar PCI DSS, FIPS 140-2, ANSI<br>✓ No tiene el módulo HSM para certificación y generación de claves.<br>✓ Depende del Host para el envió de claves.<br>✓ Costo dispositivo con mantenimiento anual es de USD 86.652 |
| **EFTSec** | • Fácil de administrar<br>• Capacidad de cifrar una porción del mensaje o su totalidad<br>• Utiliza el estándar de la industria HSM (Hardware Security Module) para el cifrado y descifrado de datos transaccionales que proveen validación en entornos FIPS 140-2, Nivel 3.<br>• Soporte de administración de llaves con el estándar HSM<br>• Elimina el costo del proceso manual de cargas de llaves<br>• Es una solución Multivendor.<br>• No requiere de hardware y software adicional. | ✓ Es una solución Multivendor para cualquier marca de cajero.<br>✓ Presenta el módulo HSM para generación y certificación de claves.<br>✓ Protocolo de comunicación TCP/IP y SNA.<br>✓ Ingreso de Claves de cifrado de forma manual.<br>✓ Costo y mantenimiento anual del dispositivo es USD 98.267 |

## 3.3 SELECCIÓN DE LA ALTERNATIVA PARA EL PROCEDIMIENTO DE GENERACIÓN DE LLAVES DE CIFRADO

Para la restructuración de la generación de llaves de cifrado, se analizaron cuatro alternativas a partir de su funcionalidad, especificaciones, estándares, requisitos de hardware y software; para lo cual, se determinó que la alternativa más factible es el dispositivo Cryptosec-RKL; teniendo en cuenta que es el único dispositivo de funcionalidad multivendor ATMs (Diebold, NCR, Wincor, Fujitsu, Omron, Itautec, keba…) y se integra con cualquier aplicación de core bancario que el cliente este usando.

Cada vez que el ATM requiera hacer cambio de llaves, el cajero automático solicita una nueva clave al sistema Cryptosec-RKL; el cual, se comunica a través de la red vía TCP/IP o SNA, y de forma remota realiza la activación de las llaves de cifrado.

### 3.3.1 Descripción económica de la alternativa seleccionada

Para la implementación de la solución Cryptosec-RKL (Key Remote Loading); se requieren adquirir dos (02) dispositivos como mínimo; debido a, que uno de ellos debe ser soporte del otro en la solución a implementar; el primer equipo se utiliza para la conexión en la red quien se encargara de soportar toda la red de cajeros del banco y el segundo estará conectado de forma redúndate para dar soporte si el principal presenta alguna falla y automáticamente quedará activo.

No obstante, se deben adquirir las licencias de llaves de cifrado; y estás se adquirirán de acuerdo al número de cajeros con que cuenta la entidad financiera. Así mismo el mantenimiento de los dispositivos será del 15% del valor de adquisición ver tabla 10

**Tabla 10**: Descripción económica de la alternativa seleccionada

| DESCRIPCIÓN | CANTIDAD | USD |
|---|---|---|
| **Cryptosec-RKL** | 2 | 163.200 |
| **Licencias Llaves cifrado** | 1 | 20.000 |
| **Implementación y Capacitación** | 1 | 70.000 |
| **Mantenimiento** | 2 | 24.480 |
| **TOTAL** | | 277.680 |

Fuente : Propia de los autores

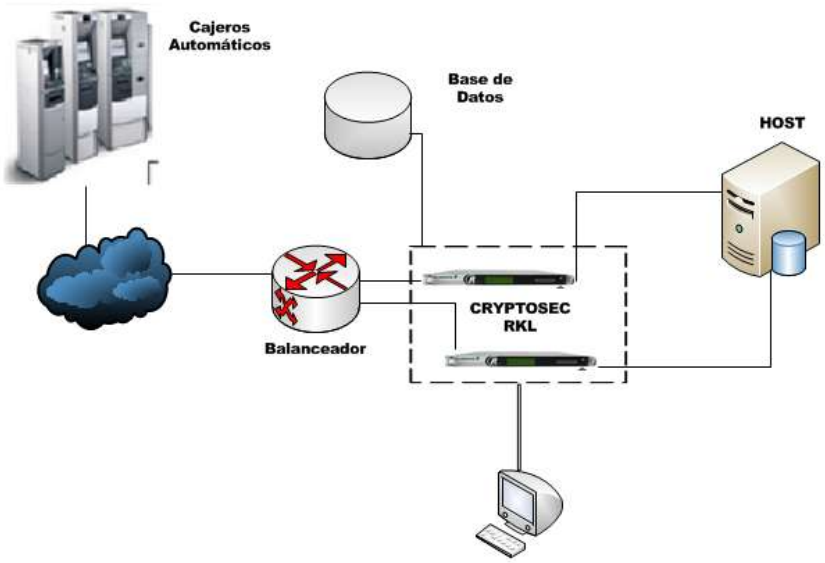
### 3.3.2 Arquitectura de diseño alternativa seleccionada

La plataforma Cryptosec-RKL recibirá las peticiones de la carga de la clave inicial procedentes de los cajeros electrónicos de la red de oficinas del Banco, seguido a

esto se llevará a cabo el proceso de autenticación mutua entre el cajero y la solución RKL siguiendo el esquema definido para cada fabricante, posteriormente se establece una sesión segura para enviar la correspondiente clave inicial de este cajero.

A partir de este momento el cajero electrónico estará en condiciones para iniciar operaciones contra el Host de la manera habitual sin necesidad de dialogar más con la solución RKL ver figura 5.

**Figura 5**: Arquitectura de diseño alternativa seleccionada




Fuente: Propia de los autores

# 4. DISEÑO DEL NUEVO PROCEDIMIENTO DE GENERACIÓN DE LLAVES DE CIFRADO MEDIANTE CRYPTOSEC-RKL

## 4.1 OBJETIVO

Establecer el nuevo procedimiento para la generación de llaves de cifrado de forma automática para cajeros electrónicos en Colombia, y lograr la confidencialidad, integridad, disponibilidad, y evitar el no repudio de las transacciones en los mismo; afianzando el cumplimiento de las normas de seguridad establecidas en las circulares externas 052 de 2007 y 022 de 2010 emitido por la Superintendencia Financiera de Colombia y la norma de seguridad de datos PCI versión 2 de Octubre de 2010.

## 4.2 ALCANCE

La habilitación de los servicios del cajero electrónico será de forma automática; donde la comunicación entre el ATM y host del banco será establecido por una autenticación del hardware implementado en la solución.

## 4.3 DEFINICIONES

- **ATM:** Cajero Automático, por sus siglas en inglés AUTOMATIC TRANSACTION MACHINE.
- **CCF:** Coprocesador criptográfico del host.
- **CDat:** Clave DES de cifrado de datos para operativa on line
- **CRIPTOGRAMA**: Resultado de aplicar una técnica de cifrado sobre un texto, asegurando la confidencialidad del mismo.
- **CGR:** Centro de Gestión de Red.
- **COMPONENTE**: Corresponde a una de las partes que conforman el Criptograma.
- **CP:** Clave DES de cifrado de PIN para operativa on line
- **DES:** Algoritmo estándar de encripción actualmente utilizado en la red de cajeros automáticos
- **3DES:** Triple DES algoritmo que hace triple cifrado del DES, nuevo estándar de cifrado, fortalece el sistema de seguridad en la red de cajeros automáticos (requerimiento mandatarios de las franquicias).
- **EPP:** Teclado con sistema de cifrado de claves propia utilizados por los ATM´s como los PIN PAD´s
- **IK:** Clave DES inicial, sólo se usa para proteger el intercambio de TK
- **KCV:** Valor de control de la clave

- **LLAVE DE RESPALDO:** Juego de componentes de respaldo, disponibles en la **MAC:** Clave DES de generación de MAC para operativa on line oficina para ser instalados en el cajero automático cuando sean requeridos
- **PKH PRH:** Pareja de claves pública/privada de host
- **RKL:** Remote Key Loading
- **SITE:** Lugar de instalación del cajero automático.
- **SOAC:** Subgerente Operativo y Apoyo Comercial.
- **TES:** Tecnología, Explotación y Soporte.
- **TK:** Clave DES de transporte de claves entre host y autoservicio
- **TKE:** (Trusted Key Entry) Dispositivo de Seguridad Basado en Hardware que permite la generación segura de componentes de cifrado.

## 4.4 RESPONSABLES

| GRUPO IMPLICADO | ACTIVIDAD |
|---|---|
| **Administrador de Seguridad** | Adquirir e implementar Infraestructura para la solución |
| **Gestión y Desarrollo** | Desarrollos en Host para soportar la nueva implementación |
| **Infraestructura Tecnología** | Adquirir y homologar la nueva solución |
| **Proveedores Cajeros** | Verificar y ajuste las especificaciones del los cajeros. |

## 4.5 RECURSOS

Los recursos necesarios para la implementación del siguiente procedimiento para la generación de llaves de cifrado para cajeros electrónicos de forma automática son los siguientes:

Físicos

- Cajero automático
- Infraestructura tecnología del banco
- Host
- Generador de llaves de cifrado (Cryptosec-RKL)

Humanos

- Líder del Proyecto
- Funcionario de seguridad lógica
- Jefe de comunicaciones
- Ingenieros de campo de la marca del cajero
- Administrador de servidores

Tecnológicos

- Área de comunicaciones

## 4.6 PROVEEDORES Y ENTRADAS

| PROVEEDORES | ENTRADAS |
|---|---|
| **Superintendencia Financiera de Colombia** | Decretos<br>Circulares<br>Procedimientos<br>Manuales<br>Políticas |
| **Franquicia MASTERCARD** | Circulares<br>Políticas |
| **Franquicia VISA** | Circulares<br>Políticas |
| **ASOBANCARIA** | Circulares<br>Manuales<br>Políticas |
| **Empresa de cajeros** | Cajeros Electrónicos<br>Procedimientos<br>Manuales<br>Políticas |
| **Ente certificador contratado por el Banco** | Certificados de Firma Digital |

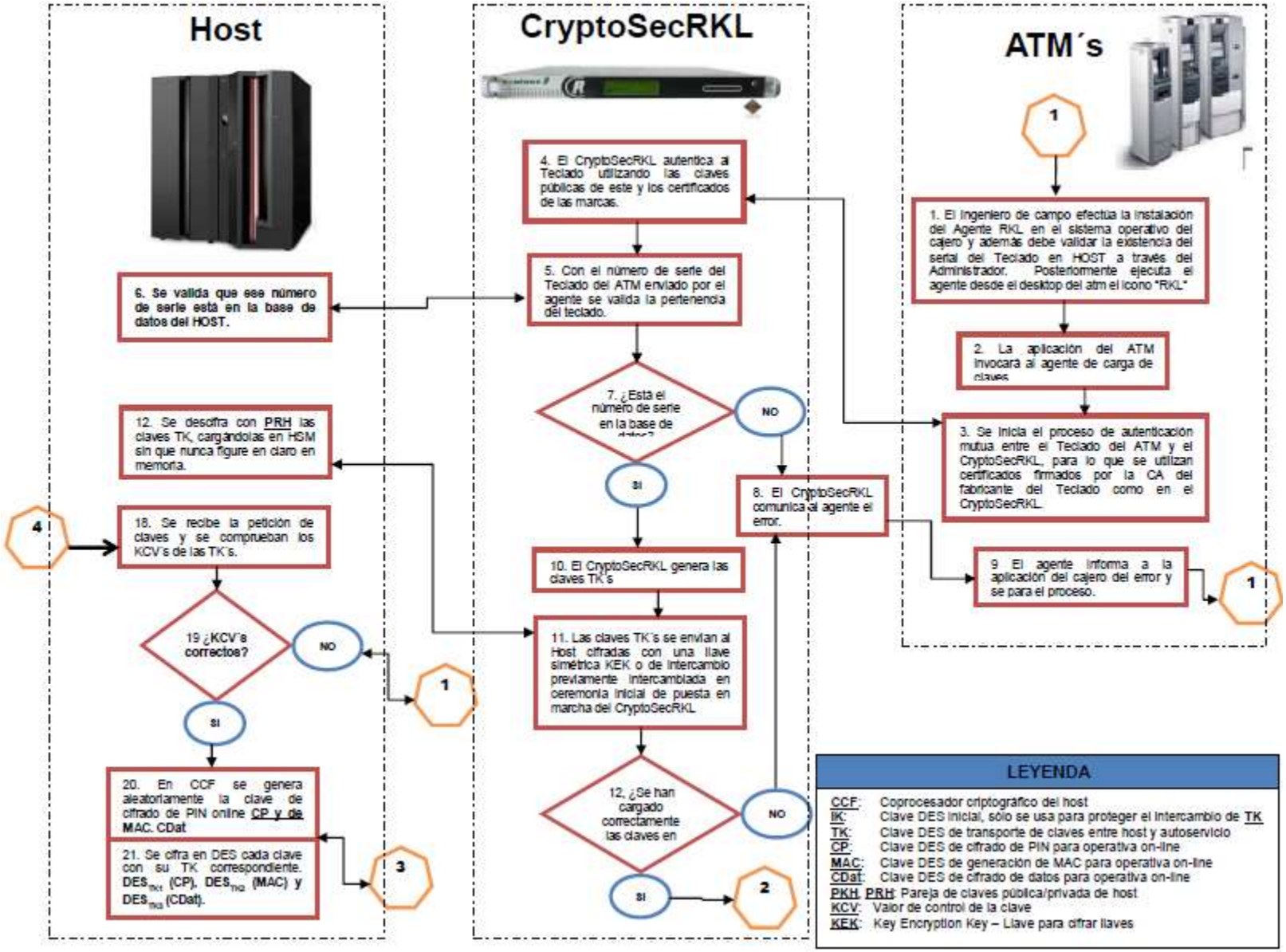
## 4.7 CLIENTES Y SALIDAS

| CLIENTES | SALIDAS |
|---|---|
| **Empresa de cajeros** | Servicio transaccionales |
| **Clientes del Banco** | Entrega de tarjeta crédito y débito<br>Habilitación de servicios en el cajero electrónico |

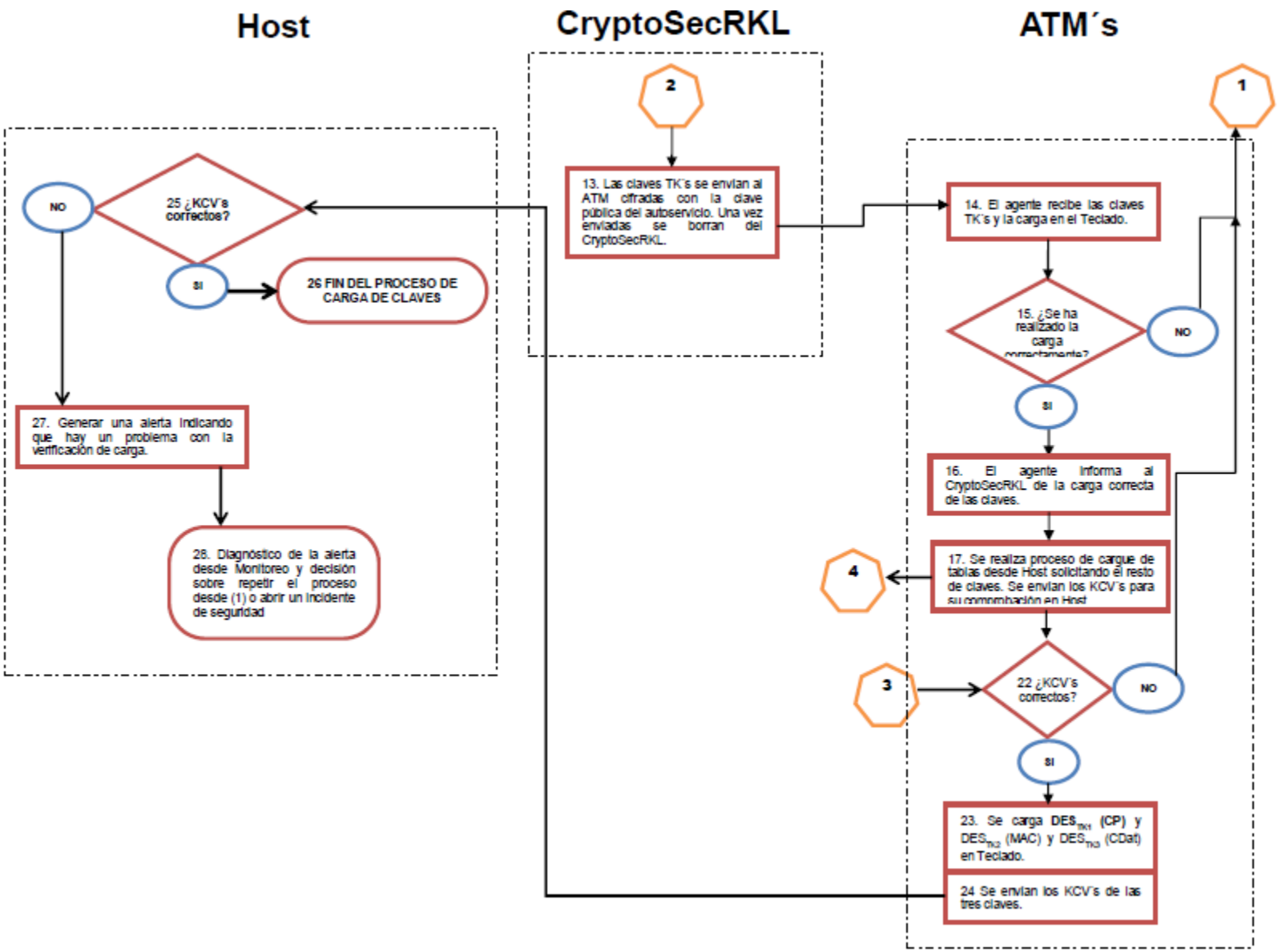
## 4.8 DIAGRAMA DE FLUJO

El diagrama de flujo para el nuevo procedimiento de generación de llaves de cifrado para la activación de los servicios del ATM a través de carga remota; en este diagrama podemos observar como es el dialogo entre el cajero automático, el dispositivo Cryptosec-RKL y el host como se podrá observar en la figura 6.

**Figura 6:** Diagrama de flujo nuevo procedimiento de generación de llaves de cifrado de forma remota




Fuente: Propia de los autores




Fuente: Propia de los autores

## 4.9 DESCRIPCIÓN DEL DIAGRAMA DE FLUJO NUEVO PROCEDIMIENTO DE GENERACIÓN DE LLAVES DE CIFRADO DE FORMA REMOTA

Inicialmente el ingeniero de campo debe realizar la activación del agente RKL en el sistema operativo del cajero automático y la aplicación del ATM invocará al agente de carga de claves para que se inicie el proceso de autenticación mutua entre el teclado del ATM y el CryptoSec-RKL, para lo que se utilizan Certificados de Firma Digital de la CA del fabricante lo que permitirá que el agente se comunique con Cryptosec-RKL enviando los datos del serial del teclado y el código del cajero; con lo cual, Cryptosec-RKL solicita al HOST se verifique en la base de datos si la información de los seriales de los dispositivos existen registrados o no; dado el caso que no existieran los dispositivos registrados el dispositivo Cryptosec informar al agente RKL para que detenga el proceso y el ingeniero de campo deberá generar el incidente de seguridad al área encargada.

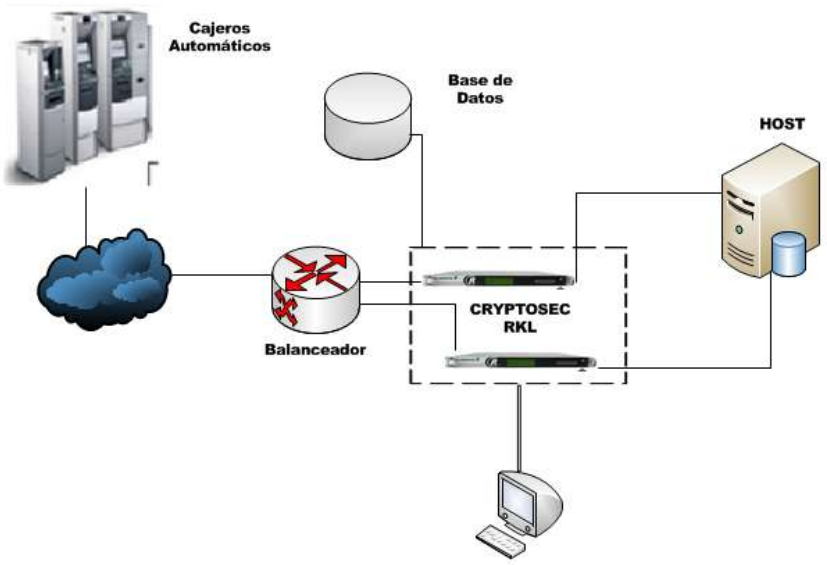
Cuando Cryptosec-RKL tiene la confirmación de que el cajero se encuentra registrado en la base de datos se envía la llave inicial de cifrado al HOST y a la vez lo remite al cajero para que quede guardado en el teclado en su módulo HSM (Hadware Security Module); luego de la activación el cajero solicita al HOST la llaves de cifrado del PIN para que inicie proceso de funcionamiento ya en esta etapa la comunicación Cryptosec-RKL no está conectado con el HOST y el ATM y finalizara todo el proceso de la carga de claves exitosamente; dado el caso que no se efectuara el envío de la carga de claves de configuración del PIN el ingeniero de campo deberá generar el incidente de seguridad al área encargada.

## 4.10 TOPOLOGÍA DE RED PARA GENERACIÓN DE LLAVES DE CIFRADO DE FORMA REMOTA MEDIANTE CRYPTOSEC-RKL

El servidor Cryptosec-RKL recibirá peticiones procedentes de los ATM para la carga de la clave; finalizada la sesión de transmisión de la clave inicial para el autoservicio en cuestión, éste estará en condiciones para iniciar operaciones contra el Host de la manera habitual sin necesidad de dialogar nunca más con el Servidor Cryptosec-RKL. En estos dos últimos supuestos, el proceso de petición de carga de claves será lanzado de nuevo por la aplicación de Autoservicio, de forma automática y transparentemente para el personal técnico o de la oficina.

Una vez completado el proceso de carga de la clave inicial por cada cajero inicializado, la aplicación de autoservicio comunicaría la nueva condición del cajero como “inicializado” a la solución de gestión de red como se muestra en la figura (ver figura 7).

**Figura 7**: Topología de red RKL




Fuente: Propia de los autores

## 4.11 COSTOS DE LA IMPLEMENTACIÓN

Para la implementación de la solución Cryptosec-RKL (Key Remote Loading); se requieren adquirir dos (02) dispositivos como mínimo; debido a, que uno de ellos debe ser soporte del otro en la solución a implementar; el primer equipo se utiliza para la conexión en la red quien se encargara de soportar toda la red de cajeros del banco y el segundo estará conectado de forma redúndate para dar soporte si el principal presenta alguna falla y automáticamente quedará activo.

No obstante, se deben adquirir las licencias de llaves de cifrado; y estás se adquirirán de acuerdo al número de cajeros con que cuenta la entidad financiera. Así mismo el mantenimiento de los dispositivos será del 15% del valor de adquisición ver tabla 11

**Tabla 11:** Costo de la implementación

| DESCRIPCIÓN | CANTIDAD | USD |
|---|---|---|
| **Cryptosec-RKL** | 2 | 163.200 |
| **Licencias Llaves cifrado** | 1 | 20.000 |
| **Implementación y Capacitación** | 1 | 70.000 |
| **Mantenimiento** | 2 | 24.480 |
| **TOTAL** | | 277.680 |

Fuente: Propia de los autores

# RECOMENDACIONES

- Todos los cajeros automáticos a nivel nacional, deben contar con un mecanismo de carga automática de llaves de cifrado para garantizar la confidencialidad e integridad de la llave maestra, mediante la utilización de módulos de seguridad Tamper-Resistant y Tamper-Responsive, en cuya memoria protegida, se procesan todos los cálculos criptográficos necesarios para dotar el sistema de carga remota de claves de todas las garantías de confidencialidad, integridad y no-repudio.

- Todos los cajeros electrónicos que sean adquiridos por la entidad financiera deben contar con un sistema de autenticación del dispositivo EPP (Encryption Pin Pad); y ser compatible con tecnología basada en HSM (Hardware Security Module); para evitar costos adicionales en la adquisición de nuevos dispositivos que lo hagan compatible con la solución.

- Según la norma PCI, las llaves cifrado se deben cambiar una vez al año; siendo responsabilidad de las entidades financieras realizar el monitoreo y cambio de llaves para cumplir con lo establecido.

- Es indispensable que la alternativa de solución a seleccionar proporcione un conjunto de aplicaciones que permita realizar todo el proceso de generación de llaves de cifrado de forma automática y se adapte al hardware existente en el core bancario.

- Todas las configuraciones en el sistema operativo del cajero debe ser ejecutado exclusivamente por el fabricante de cada uno de los ATM’s adquiridos por las Entidades Financieras.

- Es pertinente que las entidades tomen las medidas adecuadas y necesarias para mitigar el fraude en las transacciones electrónicas, según lo establecido por la Superintendencia Financiera.

# CONCLUSIONES

- Los sistemas utilizados por el sector financiero y los medios de pago constituyen un entorno comprometido con la seguridad, tanto en sus procesos como en sus operaciones transaccionales; para lo cual la banca cumple con los lineamientos mínimos establecidos por la Superintendencia Financiera Colombiana expuestos circulares externas 052 de 2007 y 022 de 2010 y la norma de seguridad de datos PCI versión 2 de Octubre de 2010, para lograr el objetivo de confidencialidad, integridad y no repudio de las transacciones electrónicas y así ofrecer a sus clientes un esquema de seguridad contra el fraude.

- La banca del sector Financiero Colombiano cumple con los lineamientos mínimos establecidos por la Superintendencia Financiera Colombiana expuestos en la circulares externas 052 de 2007 y 022 de 2010 y la norma de seguridad de datos PCI versión 2 de Octubre de 2010 pero no ofrece a sus clientes un esquema de seguridad contra el fraude financiero presencial.

- El envío de la solicitud llaves de cifrado del ATM se realiza a través del correo electrónico institucional, sin utilizar un sistema de correo seguro; esto permite que terceras personas intercepten la comunicación y puedan leer la información contenida en el mensaje.

- La generación de llaves de cifrado para la activación de los servicios del ATM son generadas por dos (02) custodios; los cuales son seleccionados aleatoriamente de la base de datos del personal de la entidad financiera; quienes a su vez se encargan de imprimir y enviar los componentes a través de correo institucional o por la empresa de mensajería contratada por el banco a la oficina solicitante.

- El sobre donde se almacenan cada uno de los componentes de las llaves de cifrado no son seguros; debido a que la forma de sellado se hace con pegamento de oficina para ser enviados a través de correspondencia certificada.

- Para la activación de los servicios del cajero automático el ingeniero de campo y el subgerente de la oficina deberán tener acceso al sistema operativo del ATM para el ingreso de las llaves de cifrado; por lo cual este proceso genera inseguridad a la información que se encuentra almacenada en el disco duro de la máquina.

- Hasta ahora el sistema tradicional de carga de las llaves de cifrado en los cajeros se venía realizando de forma manual; para poder automatizar este

proceso y ayudar a las entidades financieras a minimizar costos; las franquicias VISA y MASTERCARD, han definido estándares para la carga remota de llaves de cifrado mediante la utilización de criptografía de llave pública, dentro de un marco de aceptación universal.

- El servidor criptográfico de la solución es un dispositivo multi-vendor que permite la comunicación con cualquier fabricante de cajero electrónico (Diebold, NCR, Wincor, Fijitsu etc.)

- Al realizar la reestructuración del procedimiento actual para el ingreso de las llaves de cifrado; permite que los componentes para la activación de los servicios del cajeros se establezcan de forma remota; por lo cual se mitiga el fraude presencial en los ATM's logrando con esto la confidencialidad, integridad y evitar el repudio de las transacciones electrónicas.

- Para el caso estudio se tuvieron en cuenta cuatro (04) alternativas de solución (Futurex Series RKMS, Cryptosec-RKL, ProRKL Wincor Nixdorf y EFTSec); las cuales proporcionan las características necesarias para el diseño del nuevo procedimiento de generación de llaves de cifrado de forma remota.

# WEBGRAFIA


ESPINOSA RODRÍGUEZ, Francisco. Seguridad en operaciones financieras. Superintendencia Financieras de Colombia. Bogotá D.C. Agosto 2012. Disponible en Internet: http://www.sse.com.co/fraude-financiero-

FUTUREX COMPANY. Certificate Authority Server. Estados Unidos, Enero 2011. Disponible en Internet: http://www.futurex.com/products_general_caserver.asp

IGVANOVA, Velianna, RODRIGUEZ CABRERO, Jesús y GORDO, José Alberto. Visión de conjunto y características técnicas de Cryptosec-RKL. Madrid. Editado por Realsec. Febrero 2010. Disponible en Internet: http://www.realsec.com/pdfProEs/Cryptosec-RKL.pdf

PANDAID, Soluciones C.A. EFT Transaction Security (EFTSec) Conectividad. Venezuela, 2012. Disponible en Internet: http://www.pandaid.com/eftsec/

PÉREZ ARBESÚ, Lizzette Beatriz. Hallazgos sobre un estudio de PCI y protección de datos. Computerworld. México D.F. Editor at Ediworld SA de C.V. Octubre 26 de 2012. Disponible en Internet: http://www.computerworldmexico.mx/Articulos/25950.htm?goback=.gde_128300_member_179337052#

RAMÍREZ DE RINCÓN, Marta Lucía. Tecnología e innovación: Impacto en la competitividad. Bogotá D.C. Abril 2010. Disponible en Internet: Biblioteca virtual Luis Ángel Arango http://www.banrepcultural.org/blaavirtual/ciencias/sena/cursos-de-capacitacion/politicanal/politica3.htm

WINCOR NIXDORF International GmbH. ProRKL Central master key distribution and loading in self – service nerworks. Germany. Printed in Germany, January 2006. Disponible en Internet: http://www.wincor-nixdorf.com/internet/site_ASP/ASP/Products/Software/Banking/SecurityProcess/RKL/RKL.html

# BIBLIOGRAFÍA


DICCIONARIO DE INTERNET. Madrid, Editorial Complutense S.A. 2002.

GALENDE DÍAZ, Juan Carlos. Criptografía historia de la escritura cifrada. Madrid, Editorial Complutense, S.A. 1ª Edición, 1995.

HERRERA PÉREZ, Enrique. Tecnologías y redes de transmisión de datos. México D.F, Editorial Limusa S.A Grupo Noriega Editores, 2003.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana para la Tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información (SGSI), requisitos. Bogotá D.C., ICONTEC, 2006. NTC-ISO/IEC 27001.

INSTITUTO COLOMBIANA DE NORMAS TÉCNICAS. Norma Técnica Colombiana para la presentación de tesis, trabajos de grado, y otros trabajos de investigación. Bogotá D.C., ICONTEC, 2008. NTC 1486.

RAMOS ALVAREZ, Benjamín y RIBAGORDA CARNACHO, Arturo. Avances en criptografía y seguridad de la información. Madrid, Ediciones Díaz de Santos S.A., 2004.

STALLINGS, William. Cryptography and Network Security: Principles and Practice, 5th Edition Ilustrada, Prentice Hall, 2010.

SUPERINTENDENCIA FINANCIERA, Circular Externa 052. Bogotá D.C, 2007.

TRIGO CHACÓN, Manuel. Multinacionales, globalización y terrorismo. Madrid (España) Editorial Visión Libros, 2004.