
# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

## CIFRADO DE TRANSACCIONES FINANCIERAS EN CAJEROS AUTOMÁTICOS

## INFORME DE ACTIVIDADES PROFESIONALES

QUE PARA OBTENER EL TÍTULO DE:

## INGENIERO EN COMPUTACIÓN

P R E S E N T A :

**ROGELIO NOVA PAREDES**

ASESOR ACADÉMICO:
**M.C. MARÍA JAQUELINE LÓPEZ BARRIENTOS**

ASESOR LABORAL:
**ING. EDUARDO CALVILLO SALAS**


MEXICO, D.F. 2015

# AGRADECIMIENTOS:


## *A mis padres:*

Por siempre estar ahí, por nunca dejar de insistir, por guiar mis pasos durante todo este tiempo. Agradezco a Dios por tenerlos, estoy muy orgulloso de ustedes.

## *A mi esposa Ada:*

Por tu apoyo incondicional, por tu amor y motivación en todo momento, tu fortaleza y esfuerzo es admirable. Eres el motor de esta familia. Gracias muchas gracias por todo, ¡mi amor!

## *A mis hijos, Valentina y Eduardo:*

Ustedes son el motor que me impulsa a seguir adelante cada día, llenan de alegría y dan luz a mi familia, sus pasos me llenan de orgullo y por ustedes siempre lucharé. Agradezco a Dios por la dicha de ser su padre.

## *A mis hermanos:*

Siempre juntos y principales cómplices en muchas aventuras y travesuras, ejemplos a seguir. Sus logros me motivan a seguir adelante. Gracias por su apoyo incondicional desde siempre.

Gracias a la Universidad Nacional Autónoma de México que a través de la Facultad de Ingeniera me brindó un lugar y la oportunidad de conocer, aprender y crecer como ser humano. Gracias a ella conocí y tengo los mejores amigos de la vida. Muchas gracias a la **M.C. María Jaqueline López Barrientos** por su tiempo y esfuerzo dedicado para poder concluir este proyecto.

# Contenido

# INTRODUCCIÓN

# INTRODUCCIÓN

La información se ha convertido en los últimos años en el activo más importante para muchas organizaciones y mantener su adecuada protección es todo un reto. Las organizaciones también tienen la necesidad cada vez mas de interactuar o interconectarse entre sí y muchas de ellas compartir información, esto conlleva a la posibilidad de exponer la información a una variedad más amplia de amenazas y vulnerabilidades.

La información, no importando cuál sea la forma en que se presente, medios electrónicos, impresos o escritos, deberá siempre estar protegida adecuadamente. La protección de la información se ha convertido en un nicho muy importante para muchas compañías tecnológicas, que han comenzado a buscar diversas formas de proteger la información. Empresas como IBM, RSA, EMC, SYMANTEC, McAfee, entre otras, han invertido esfuerzos y dinero para obtener soluciones que protegen la información desde diferentes ópticas y escenarios.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas, para asegurar la continuidad del negocio; minimizar los daños y maximizar el retorno de las inversiones y las oportunidades del negocio.

La seguridad de la información se consigue implantando y supervisando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software.

Para una organización es esencial identificar sus requisitos de seguridad, y para esto existen tres fuentes principales:

1. Valoración o análisis de riesgos.
2. Buenas prácticas, marcos normativos y estándares de seguridad, marcos legales.
3. Principios y objetivos en el procesamiento de la información para apoyar su operación.

Basados en los requisitos anteriores y con la finalidad de mantener la confidencialidad, la disponibilidad y la integridad de la información, así como de disminuir los costos en el procesamiento de medios de pagos (transacciones financieras) los principales bancos de México BBVA Bancomer y CITI Banamex unen fuerzas, y en el año de 1999 forman E-Global (Servicios Electrónicos Globales). Constituída como una empresa de servicios financieros y medios de pagos, siendo en ese entonces, el segundo procesador de medios de pagos en México. Para el año 2006 E-Global se convierte en el principal procesador de medios de pagos de México al procesar cerca de 4 millones de transacciones tan solo en la temporada navideña (Diciembre 2006 –Enero 2007).

Dado el volumen transaccional logrado en el año 2006 las principales marcas como VISA y MasterCard exigen a E-Global obtener una certificación llamada Payment Card Insdustry - Data Security Standar o PCI DSS por sus siglas en inglés.

PCI – DSS son las normas de seguridad de datos de la industria de tarjetas de pagos. Las empresas fundadoras de esta organización son American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa, Inc. quienes también fundan la organización PCI Security Standards Council, foro abierto destinado a la difusión y la aplicación permanente de las normas de seguridad para la protección de datos de cuentas a nivel mundial. La norma proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas.

Estas se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen negocios, procesadores, adquirentes, entidades emisoras y proveedores de servicios como las que se muestra en la figura 1, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas.


Fig. 1 Marcas patrocinadores de PCI Security Standards

El estándar constituye un conjunto de 12 dominios que protegen los datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos. De forma general a continuación en la tabla 1 se describen los 12 controles:

TABLA 1. CONTROLES DE PCI

| Descripción general de controles PCI | |
|---|---|
| **Desarrollar y mantener una red segura** | 1. Instalar y mantener una configuración de firewall para proteger los datos de la tarjeta.<br>2. No use contraseñas de sistemas y parámetros de seguridad de fábrica. |
| **Proteger los datos del titular de la tarjeta** | 3. Proteja los datos del titular de la tarjeta que fueron almacenados.<br>4. Cifrar la transmisión de los datos del titular de la tarjeta en redes públicas abiertas. |

| | |
|---|---|
| **Mantener un programa de administración de vulnerabilidades** | 5. Utilizar y actualizar con regularidad los programas o software de antivirus.<br>6. Desarrollar y mantener sistemas y aplicaciones seguras. |
| **Implementar medidas solidas de control de acceso** | 7. Restringir el acceso a los datos del titular de la tarjeta.<br>8. Asignar un ID exclusivo a cada persona que tenga acceso a un recurso de TI.<br>9. Restringir el acceso físico a los datos del titular de la tarjeta. |
| **Supervisar y evaluar las redes con regularidad** | 10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.<br>11. Pruebe con regularidad los sistemas y procesos de seguridad. |
| **Mantener una política de seguridad de la información** | 12. Mantenga una política que aborde la seguridad de la información para todo el personal. |

PCI DSS se aplica a todas las empresas u organizaciones que almacenen, procesen, o transmitan datos de los titulares de tarjetas y/o datos confidenciales de autenticación como se detalla a continuación en la tabla 2:

**TABLA 2. DATOS CLASIFICADOS SENSIBLES PARA PCI**

(Security Standar Councill, 2010)

| Datos de titulares de tarjeta | Datos confidenciales de autenticación |
|---|---|
| • Número de cuenta principal (PAN)<br>• Nombre del titular de la tarjeta<br>• Fecha de vencimiento<br>• Código de servicio | • Datos de la banda magnética o chip<br>• CAV2/CVC2/CVV2/CID – Código de seguridad de tarjeta-<br>• PIN/Bloqueos de PIN |

Para el periodo 2007-2008 E-Global en busca de la mejora continua persigue por primera vez la certificación PCI DSS, esto repreentó nuevas oportunidades para fortalecer el área de seguridad informática al igual que un gran reto y esfuerzo, sobre todo por la cantidad de controles de seguridad que implicó desarrollar, implementar y mantener.

Así los primeros controles con los que E-Global inicia su proceso de certificación en el estándar de PCI y la mejora de controles que aseguren la confidencialidad, disponibilidad e integridad de la información son:

- Monitoreo y análisis de logs.
- Monitoreo FIM
- Escaneo y análisis de parches y vulnerabilidades.
- Programa de capacitación y concientización en seguridad de la información – Security Awarness.

Para el año 2011 E-Global continúa creciendo y expandiendo servicios a nuevos clientes, este crecimiento promueve a explorar nuevos nichos en el mercado de medios pagos. Para finales del 2011 E-global empieza a vislumbrar un mercado nuevo, el mercado de cajeros automáticos, dominado actualmente por nuestra competencia directa PROSA (Promotora de servicios).

Para llevar a cabo el proyecto de cajeros automáticos se forma un equipo de trabajo, conformado por:

- **Un líder de proyecto** - Responsable de coordinar las actividades y del proyecto.
- **Dos Programadores Sénior** - Responsable de realizar las interfaces finales para usuarios.
- **Un ingeniero de arquitectura de TI** - Responsable de definir la arquitectura de TI necesaria (servidores, equipos de comunicación, seguridad perimetral).
- **Un ingeniero en Telecomunicaciones** - Responsable de implementar toda la infraestructura de comunicaciones.
- **Un especialista de seguridad informática** - Responsable de definir toda la arquitectura de seguridad y la infraestructura de cifrado.
- **Un especialista DBA sénior** - Responsable de generar las instancias y bases de datos necesarias.

La implementación de la arquitectura inicia formalmente en agosto del 2013, y para enero del 2014 se logra implementar el primer piloto de cajero. Para inicios del 2015 se tiene el objetivo de implementar aproximadamente 50 cajeros automáticos para dos clientes bancos.

# CAPÍTULO 1: Trayectoria Profesional

## 1.1 Desarrollo Profesional

Egresé de la Facultad de Ingeniería en el año 2006, incorporándome desde entonces al campo laboral, desempeñando funciones y actividades afines con la carrera, como:

- Arquitectura de computadoras
- Seguridad en redes
- Base de datos
- Programación

Adicional al conocimiento base en temas específicos sobre la carrera de ingeniería en computación, la Facultad de Ingeniería fomenta una formación que permite desarrollar en los estudiantes una capacidad de análisis y razonamiento que ayuda a resolver problemas de una manera concreta. De igual forma no podemos dejar de mencionar el aspecto social y humano de la Universidad, la cual sin duda nos da una sensibilización sobre nuestro entorno social, político y económico que se vive en la actualidad.

Esta formación sin duda me permitió incorporarme rápidamente en el campo laboral.

Después de una serie de exámenes de diversos tipos como de conocimiento, psicológicos y de razonamiento, tuve la oportunidad en el 2006 de ingresar a laborar dentro del grupo financiero BBVA Bancomer despeñando el puesto de Ingeniero Operador de Red, teniendo las siguientes responsabilidades:

- Monitoreo, configuración, administración y soporte de primer nivel a las redes de cómputo y telecomunicaciones del grupo financiero BBVA Bancomer.

- Administración de la red Internacional de Telecomunicaciones del grupo BBVA Enlaces Internacionales E1, E3.

- Administración de la Plataforma de Routers y Switchs Cisco (configuración y diagnóstico de problemas).

- Administración de redes WAN y LAN de la Institución.

- Evaluación y medición de los diferentes medios de comunicación apoyados de herramientas de monitoreo. Elaboración de reportes, estadísticas de los enlaces, seguimiento de problemas.

- Solución a problemas relacionados con la red de transporte WAN, LAN Y la red SNA de IBM, incluyendo:

-ROUTERS CISCO
-SWITCHS Y CONCENTRADORES Y ENTERASYS
-REDES ETHERNET
-REDES TOKEN RING
-SISTEMA OPERATIVO DE CONSOLAS VTAM (VIRTUAL TELECOMUNICATIONS ACCESS METHOD), SPECTRUM (SOLARIS), MANEJO DE SOFTWARE: NETVIEW (IBM TIVOLI)

- Manejo e interpretación de capturas con sniffer
  (PRO VERSION – NETWORK ASSOCIATES)

- Monitoreo y alertas en la red de cajeros y sucursales utilizando SPECTRUM (UNIX, SOLARIS) y TIVOLI NETVIEW (IBM).

En la búsqueda de mi crecimiento profesional, en el 2008 tuve la oportunidad de incorporarme a una empresa mediana pero con grandes oportunidades de crecimiento, potencial y necesidades de desarrollar e implementar nuevas tecnologías, herramientas, sistemas y procedimientos en el área de seguridad informática: Servicios Electrónicos Globales S.A. de C.V. (E-Global).

Durante los primeros dos años (2008-2010) en E-Global ocupé el puesto de Analista de Seguridad Informática, siendo mi función principal apoyar en la implementación y ejecución de los primeros monitoreos de seguridad, dentro de la Subdirección de Seguridad Informática.

A partir del 2010 y hasta la fecha ocupo el cargo de Gerente de Seguridad informática teniendo las siguientes responsabilidades:

- Promover la confidencialidad, integridad y disponibilidad de la información alineada a la estrategia institucional.

- Ejecutar y coordinar acciones pertinentes para promover el cumplimiento de la normatividad vigente en materia de políticas, procedimientos y estándares de seguridad de la información basados en una estructura documental metodológica y/o estándares o buenas prácticas de seguridad (Ej. PCI, ISO27000,COBIT)

- Verificar el cumplimiento de los estándares en las configuraciones de diferentes plataformas tecnológicas (Windows Server, UNIX, CISCO etc.)

- Llevar a cabo acciones de difusión, concientización y capacitación en materia de seguridad con el fin de lograr una operación razonablemente segura.

- Coordinar las acciones necesarias para desarrollar e implementar la arquitectura de seguridad lógica, tales como, monitoreo de logs (Envision, SNARE), monitoreo de integridad (FIM, Tripwire), correlación de eventos (SIEM) y trabajar de manera conjunta con todas las áreas de la organización para hacer enlace entre los procesos operativos, tecnológicos y de seguridad lógica.

- Planear y coordinar los programas de control de acceso vigentes en todas las plataformas tecnológicas y aplicaciones autorizadas, manteniendo esquemas de supervisión y monitoreo para detección y atención a desviaciones e incidentes para lograr una operación razonablemente segura.

- Revisión, monitoreo y seguimiento en la ejecución de los programas de control de cambios vigentes tanto en hardware como en software para identificar posibles desviaciones e incidentes que pongan en riesgo la operación.

- Ejecución de los programas de búsqueda e identificación de vulnerabilidades y actualizaciones de seguridad faltantes en las plataformas tecnológicas (NESSUS, Foundstone, Retina).

- Realizar procesos de diagnóstico de análisis de riesgos en el manejo de la información y a procesos de seguridad lógica.

- Participar en los programas de recuperación y continuidad de la operación probando los procedimientos de los procesos y servicios críticos vigentes así como la identificación de áreas de oportunidad para lograr una operación razonablemente segura y continua.

# CAPÍTULO 2: Proyectos Profesionales

A continuación se describen algunos proyectos representativos de mi quehacer profesional en los que he participado, mismos que resaltan por el reto profesional que implicó llevarlos a cabo, así como por la satisfacción y cumplimiento que le brindaron a la organización.

## 2.1. Monitoreo y análisis de logs de sistemas operativos

Con la finalidad de mantener un esquema de seguridad que permita detectar desviaciones al cumplimiento de la normatividad de Seguridad de la Información, además de cumplir con los estándares y regulaciones, tanto internos como externos, que rigen a E-Global, en diciembre del 2007 se implementa un proceso para monitorear los registros de auditoría y eventos de seguridad en los sistemas.

### Objetivo

Detectar posibles desviaciones e incidentes de seguridad que pongan en riesgo la información de la empresa, a través de la implementación de procesos y procedimientos, necesarios para realizar un monitoreo periódico de los logs de seguridad en la infraestructura de TI.

### Descripción del proyecto

El almacenamiento centralizado de logs así como el monitoreo se implementaron utilizando un software tipo SIEM (System Information Event Manager).

El punto de partida para llevar a cabo el monitoreo fue establecer qué se iba a monitorear, para esto se definieron cuatro rubros importantes: ataques, accesos, cambios y actividad. (Véase figura 2.1)

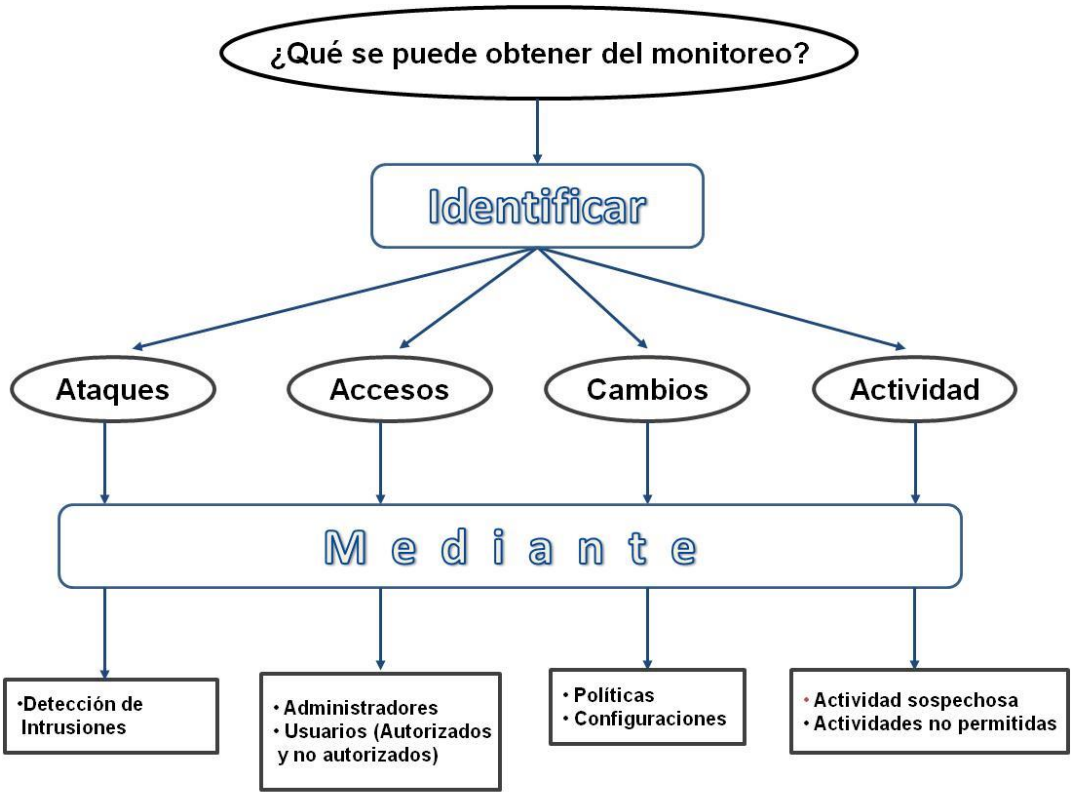



Fig. 2.1 Esquema de monitoreo

Una vez establecidos los rubros a monitorear, el siguiente paso fue establecer la matriz de eventos o logs específicos a identificar (véase fig. 2.2)

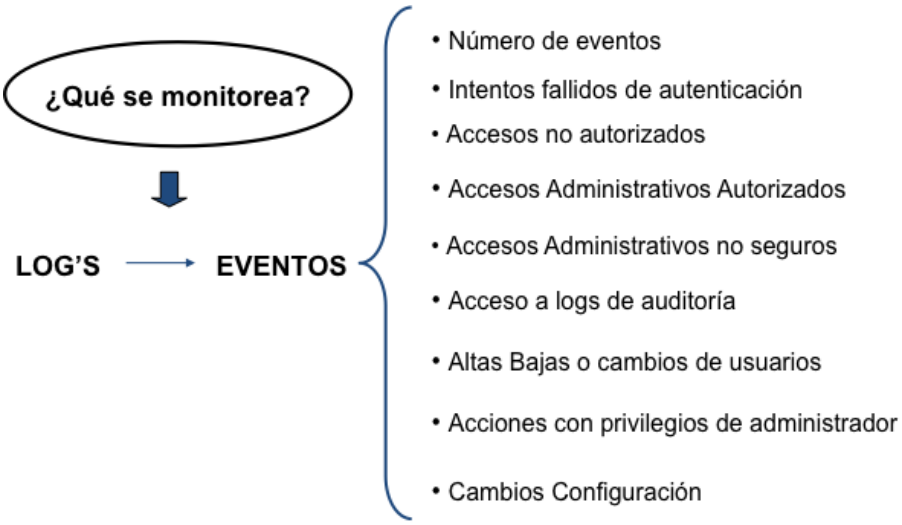



Fig. 2.2 Eventos de monitoreo

El monitoreo es de tipo detectivo/reactivo ante eventos ya realizados.

El alcance de dispositivos de la infraestructura de TI se definió tal como se aprecia en la Tabla 2.1

Tabla 2.1 Infraestructura de TI

| Cantidad | Sistema | Plataforma |
|---|---|---|
| 3 | Stratus ON/2 | Switch (linea) |
| 8 | Unix Solaris | Procesamiento Batch |
| 2 | Unix Aix | Ecommerce |
| 2 | Cisco | Ruteadores |
| 4 | Juniper | Firewalls |
| 18 | Windows | Red y Producción |
| 3 | Linux | Ldap |
| 40 | | |

## Arquitectura de la solución

Existen diversas formas de concentrar los logs, gran parte de los sistemas actuales (UNIX, CISCO, IBM, etc. entre otros) utilizan el protocolo llamado SYSLOG.

SYSLOG es el protocolo estándar utilizado para el envío de mensajes de eventos, los mensajes son enviados por el puerto 514 UDP en texto plano. El protocolo se estandarizó y se le asignó el RFC 3164.

Para la mayor parte de la infraestructura de TI de la empresa se utilizó el protocolo SYSLOG, a excepción de Windows que utiliza su propio protocolo de eventos "Eventview" a través de NTLMv2 (véase figura 2.3).

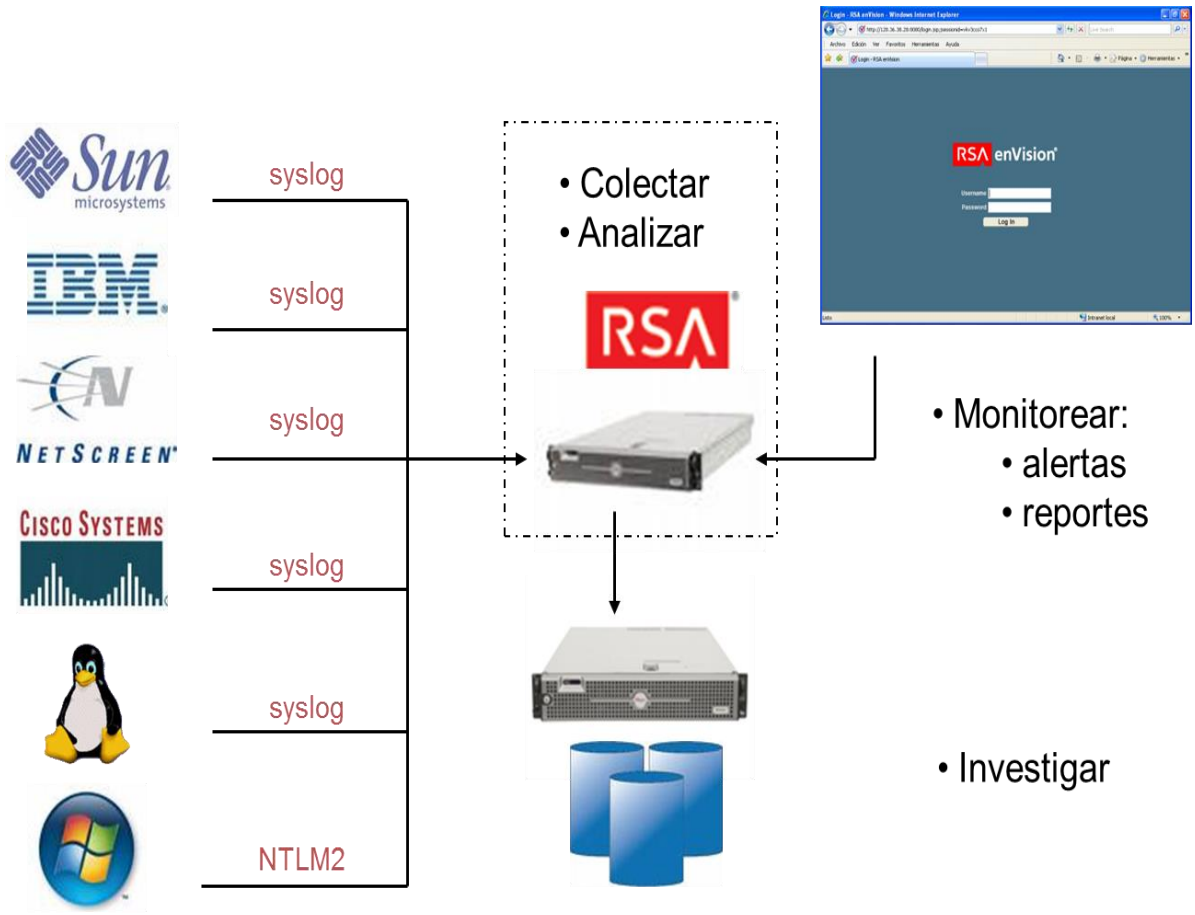



Fig. 2.3 Arquitectura de la solución

Se realizó una evaluación técnica y financiera a diferentes proveedores, la solución adquirida por la empresa fue una provista por RSA llamada EnVision y catalogada en el mercado como un SIEM o correlacionador de eventos.

EnVision es un producto de RSA certificado por PCI DSS, con lo cual garantiza el cumplimiento del estándar de seguridad.

Un correlacionar de eventos o SIEM es un sistema colector de eventos, que permite en primera instancia recolectar los logs de los equipos, esto ayuda a que los logs se almacenen en un lugar centralizado y puedan ser consultados cuando se requiera.

El segundo objetivo de implementar un SIEM es realizar una correlación de eventos para identificar posibles incidentes o desviaciones de seguridad, tras un monitoreo, en el cual se revisan los logs de sistema operativo, base de datos, firewalls, routers, entre otros, los hallazgos que son identificados se documentados y reportan como incidentes o desviaciones de seguridad. En el siguiente diagrama de flujo (véase Figura 2.4), se describen los pasos del monitoreo que se implementaron y que actualmente se llevan a cabo.

## Diagrama de flujo

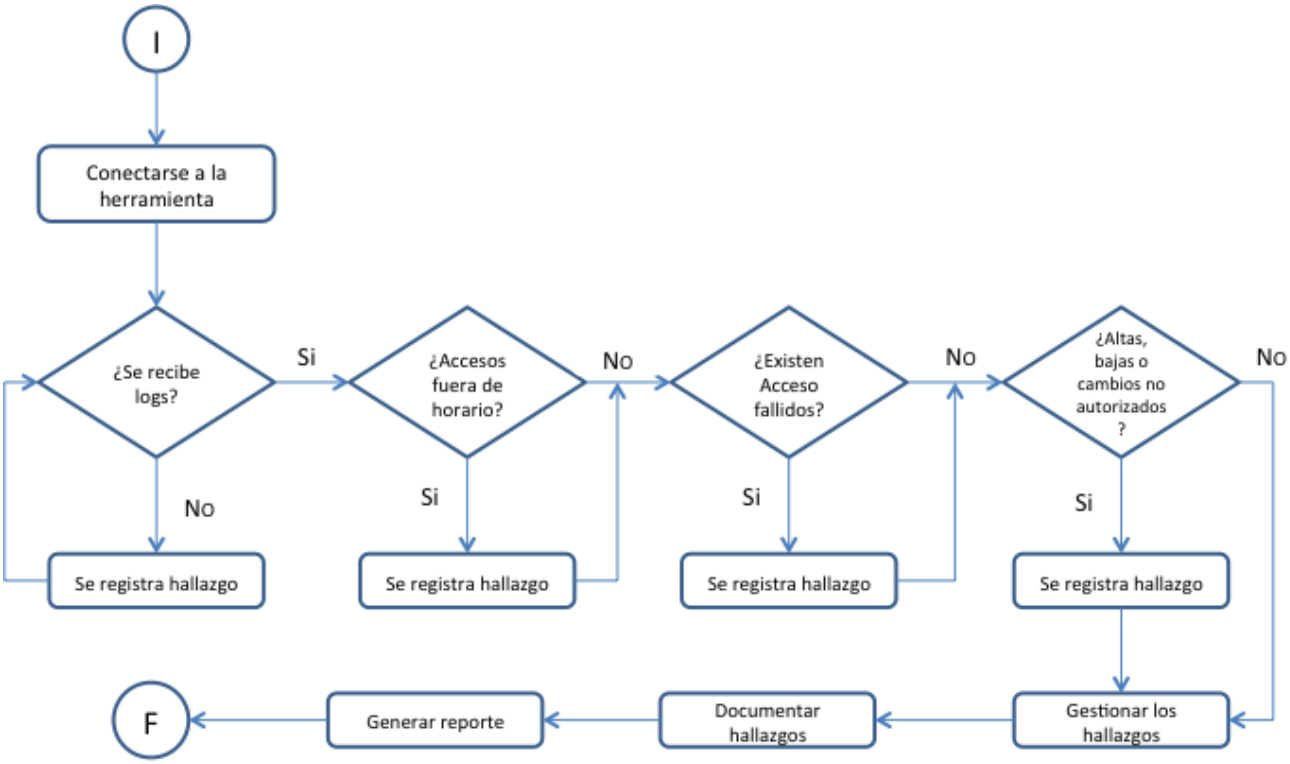



Fig. 2.4 Diagrama de flujo – Monitoreo de logs

En la Tabla 2.2 se detallan las actividades y seguimiento de hallazgos que se mencionan en el diagrama de flujo anterior (Figura 2.4 Diagrama de flujo – Monitoreo de logs).

Tabla 2.2 Descripción de actividades

| Actividad | Descripción de la actividad | Evidencia |
|---|---|---|
| • Recepción de Logs | Se verifica la recepción de logs dentro del colector de eventos | En la bitácora de se registra si la recepción de logs fue satisfactoria y la cantidad de logs recibidos |
| • Acceso fuera de horario establecido | Se registran los accesos detectados por los administradores fuera de horario laboral. | En la bitácora de monitoreo se registran los eventos detectados, se levanta reporte al administrador para justificar el ingreso. |
| • Intentos fallidos de acceso | Se busca identificar si alguna actividad sospechosa como intentos de accesos no exitosos. | Si se identifican mas de tres intentos no exitosos de acceso, se registra en bitácora y se reporta al administrador para su conocimiento y validación. |
| • Cambios no autorizados | Los cambios aplicados en los sistemas son validados y verificados por medio de los logs de sistemas. | Cuando se identifica un cambio no registrado y previamente autorizado se registra en la bitácora y se reporta al administrador para su justificación y seguimiento del hallazgo |
| • Gestionar hallazgos, documentar y cierre de reportes | Los hallazgos identificados y registrados son documentados hasta su cierre | Dentro de la bitácora de monitoreo se da seguimiento a los hallazgos hasta su cierre |

Para dar continuidad, seguimiento y tener evidencia de cumplimiento, se desarrollaron bitácoras de monitoreo, en la figura 2.5 se muestra un ejemplo de la bitácora.

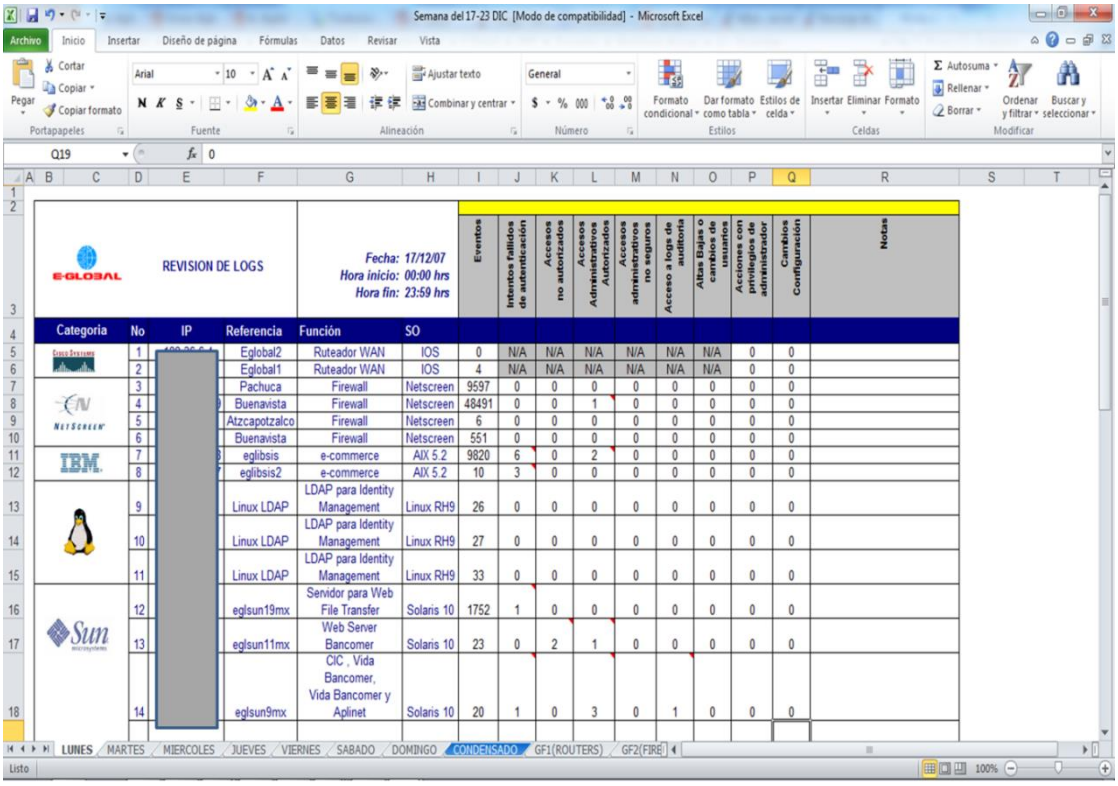



Fig. 2.5 Bitácora de monitoreo

La evidencia de hallazgos se maneja en bitácoras de registro y diferentes archivos entregables que muestran la revisión y supervisión diaria del monitoreo de logs (véase fig. 2.6).


Fig. 2.6 Fases del monitoreo

## Desarrollo en el tiempo

La puesta a punto del proyecto se dio en tres fases como se muestra en la gráfica siguiente de la figura 2.7.

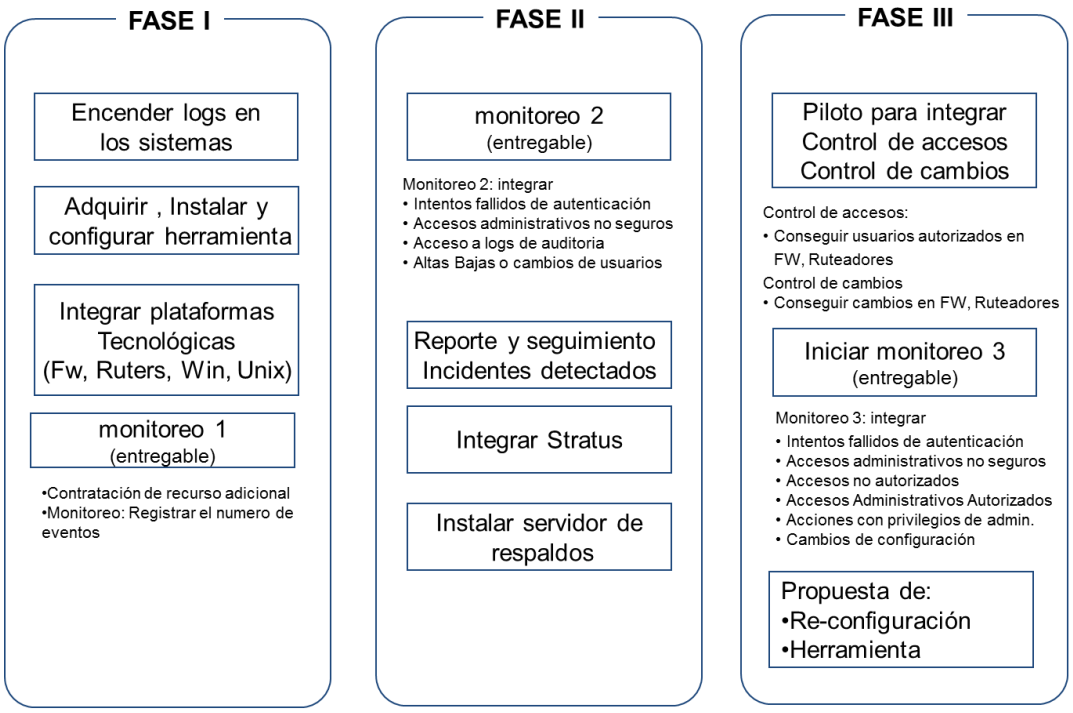



Fig. 2.7 Fases del monitoreo

### Resultados

El monitoreo de logs dio cumplimiento durante los tres primeros años a partir del 2007, desde entonces ha entrado en una mejora continua cada año, donde se ha ido optimizando el proceso, hemos crecido tanto en la infraestructura como en la plantilla de seguridad dedicada a este proceso. Se contrató personal especializado y dedicado a realizar estas revisiones.

Actualmente se monitorean alrededor de 80 dispositivos de diferente arquitectura como son UNIX, Windows, Fw, routers, por mencionar algunos.

Como mejora continua, en los próximos años, se plantea una renovación tecnológica de la herramienta de monitoreo de logs, al igual que cambios en los procedimientos con la finalidad cubrir nuevos requerimientos y estándares de seguridad.

## 2.2. Monitoreo y análisis de integridad

Con la finalidad de mantener un esquema de seguridad que permita detectar desviaciones al cumplimiento de la normatividad de Seguridad de la Información, para cumplir con los estándares y regulaciones tanto internas como externas que rigen a E-Global, en junio del 2009 se implementó un proceso para monitorear la integridad de los archivos críticos de los sistemas a nivel de sistema operativo, base de datos y aplicaciones.

### Objetivo

Implementar un software de monitoreo de integridad en todos los servidores que se encuentren en producción y en alcance de revisión PCI, estableciendo los procesos necesarios y mecanismos de monitoreo que permitan detectar cualquier cambio no autorizado en los archivos críticos de la infraestructura de TI.

### Descripción del proyecto

El monitoreo de integridad o File Integrity Monitor FIM (por sus siglas en inglés), es un control interno o proceso que realiza la validación de la integridad de archivos a nivel de sistema operativo, software de aplicación, o base de datos, usando un método de verificación entre el estado actual del archivo y un estado anterior conocido. Este método de comparación a menudo implica el cálculo de una función HASH criptográfica. Una de las funciones de un HASH es la detección de modificaciones, por lo que permite verificar la integridad del mensaje.

De manera similar al monitoreo de logs se definió el alcance sobre los sistemas que se iban a monitorear y que a la fecha se siguen monitoreando. (Véase Tabla 2.2)

Tabla 2.3 Infraestructura de TI – Monitoreo de FIM

| Cantidad | Sistema | Plataforma |
|---|---|---|
| 8 | Unix Solaris | Procesamiento Batch |
| 18 | Windows | Red y Producción |
| 26 | | |

Este monitoreo es del tipo detectivo/reactivo ante cambios ya realizados en los programas y sistemas.

El proceso de monitoreo diseñado, ayuda a obtener una validación de los cambios aplicados en los sistemas con previa autorización por parte del comité de cambios contra los cambios detectados en el monitoreo (véase figura 2.8)

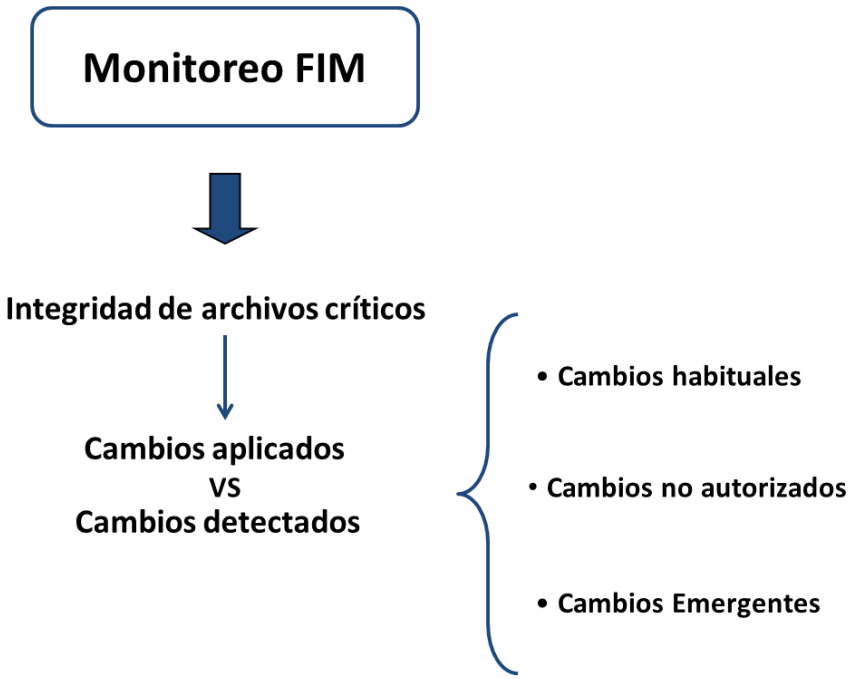



Fig. 2.8 Monitoreo FIM

## Arquitectura de la solución

La solución adquirida en ese momento por la empresa fue Tripwire, esto tras haber realizado un análisis financiero y técnico. Es una herramienta que permite realizar un monitoreo en tiempo real sobre la integridad de los archivos que se consideren a monitorear sobre los dispositivos, además de contar con las características de cumplimiento PCI DSS.

Tripwire es una herramienta que soporta diversas plataformas de TI y sistemas operativos (UNIX, Windows, AIX, Oracle, informix, por mencionar algunos), la forma de comunicación es a través de un agente que se instala en cada servidor o equipo que se desee monitorear, este agente se comunica a una consola, la cual cuenta con una interfaz web para ser accedida por el especialista de seguridad informática y se pueda llevar a cabo el monitoreo y/o las acciones requeridas como administrador de la herramienta (configuración de alerta, seguimiento a cambios, validar integridad de archivos, por ejemplo.)

A continuación se muestra en la figura. 2.9 el esquema de conexión del Tripwire para plataformas con sistema operativo Windows y UNIX.

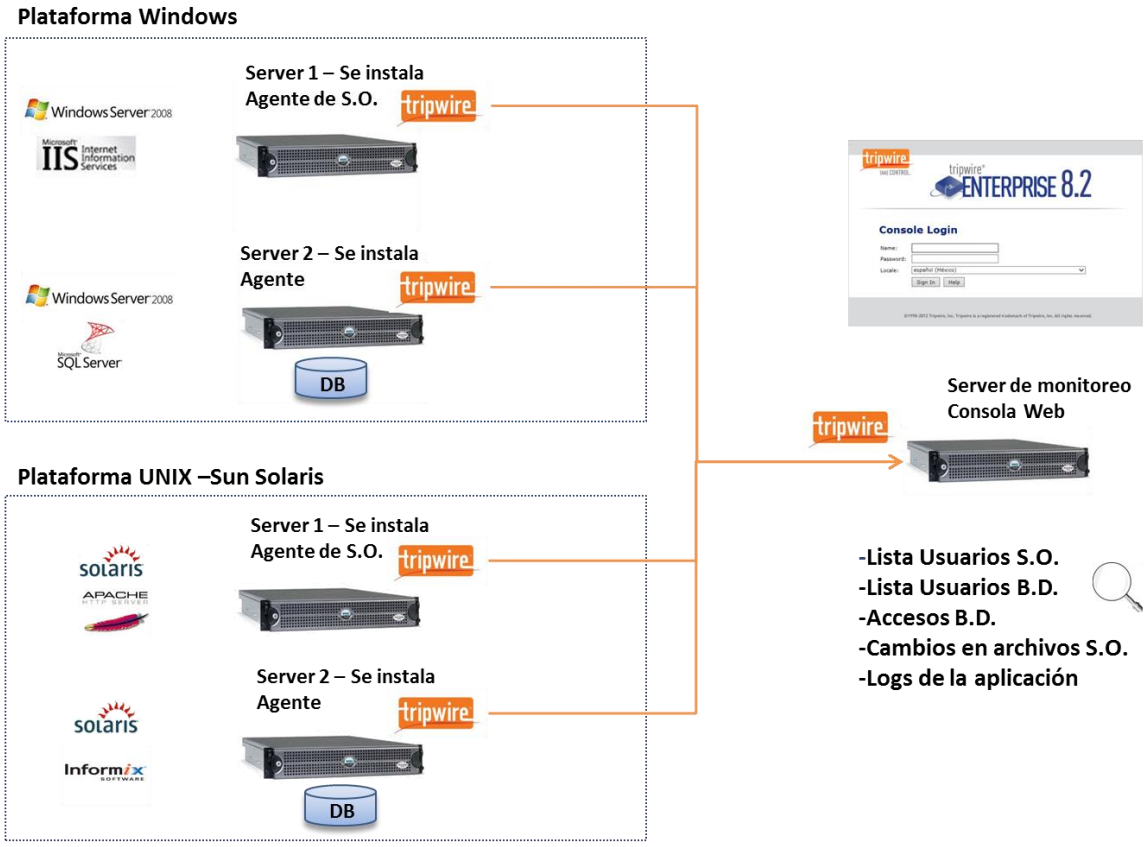



Fig. 2.9 Esquema de seguridad

Durante la instalación del agente se realizan algunas configuraciones, principalmente: el puerto de comunicación y la dirección IP de la consola, para validar la comunicación entre los agentes y la consola se realiza una prueba básica de telnet.

Si la comunicación es exitosa inmediatamente se refleja en la consola de administración del Tripwire en forma de nodo el equipo a monitorear. Se configuran y aplican las reglas de monitoreo y alertas sobre los archivos u objetos que se deseen revisar. (Véanse las figuras 2.10 y 2.11)

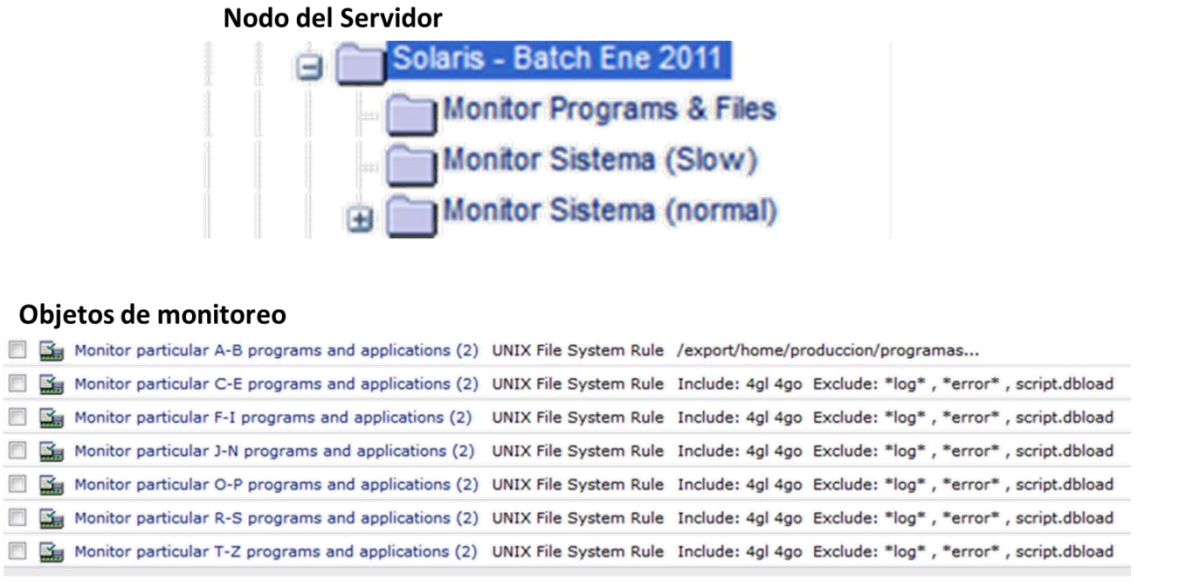



Fig. 2.10 Nodo de monitoreo


Fig. 2.11 Reglas de monitoreo

El proceso consiste en validar el estado actual del archivo u objeto contra un estado anterior conocido, si el objeto o archivo sufrió alguna modificación este cambio inmediatamente se refleja por la variación del HASH, estos cambios se verifican con los registros de cambios que se promovieron y su autorización en el comité de evaluación de cambios.

El comité de evaluación de cambios valida y verifica que los cambios aplicados en la infraestructura de TI cumplan con los requisitos necesarios para su ejecución como por ejemplo riesgo, plan de retorno, plan de ejecución, entre otro, este proceso se describe en el siguiente diagrama de flujo (Véase figura 2.12).

## Diagrama de flujo

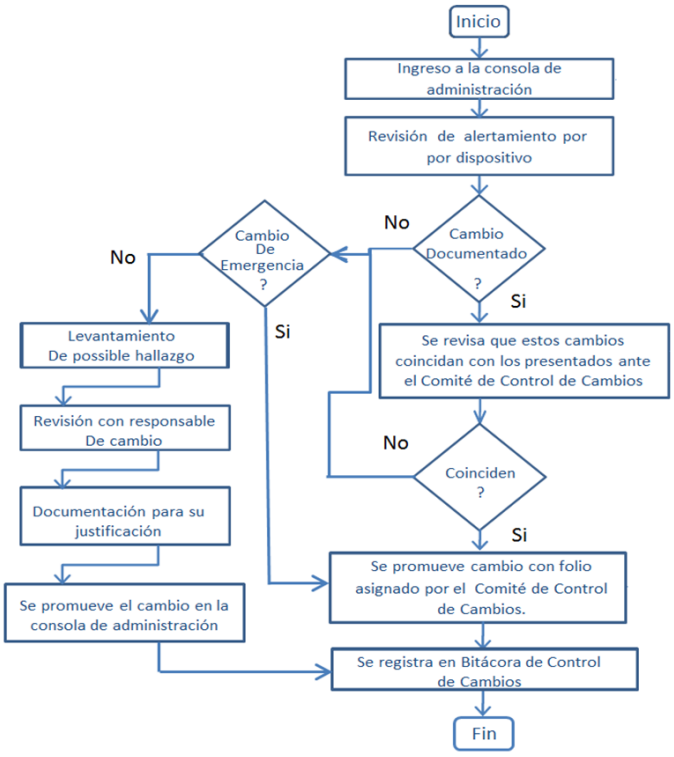



Fig. 2.12 Flujo Monitoreo FIM

Para dar continuidad, seguimiento y tener evidencia de cumplimiento, se desarrollaron bitácoras de monitoreo, en la figura 2.13 se muestra un ejemplo de la bitácora.

**Control de Cambios Monitoreo** [redacted]

| Cifras de Control | |
|---|---|
| CH | 4 |
| CA | 0 |
| CNR | 1 |
| CE | 0 |

| IP Address | Tipo | Folio Seg Inf | Estatus | Descripción | Referenica CC | Detalle |
|---|---|---|---|---|---|---|
| **SUN Solaris** | | | **Validar** | | | |
| [redacted] Sun Batch | Produccion | N/A | Habitual | Se modificaron los archivos totales y datos_con una vez que se valide que no contiene información sensitva, se eliminará del monitoreo. | N/A | Ver detalle del cambio |
| [redacted] Sun Batch | Produccion | ds-053 | Validar | Se agregaron archivos de carga dentro de la carpeta del proyecto de GFU para Nicaragua, Costa Rica, Honduras y el Salvador, siendo que durante ésta semana solamente se tenía planeado el proyecto de El Salvador. | Sin Control de Cambios | Ver detalle del cambio |
| **AIX** | | | **Validar** | | | |
| [redacted] Aix Producción | Produccion | N/A | Habitual | Se agregó y modificó un archivo del tipo xmwlm, una vez que se valide que no contiene información sensitva, se eliminará del monitoreo. | N/A | Ver detalle del cambio |
| [redacted] AIX Pre-producción | Produccion | N/A | Habitual | Se modificaron los archivos 1.hir, 2.hir y 4.hir, una vez que se valide que no contiene información sensitva, se eliminará del monitoreo. Se validó con Hector Rosas que éste archivo se modifica de manera diaria habitual debido a un proceso automático del manejador de base de datos db2. | N/A | Ver detalle del cambio |
| [redacted] AIX Pre-producción | Produccion | N/A | Habitual | Se agregó y modificó un archivo del tipo xmwlm, una vez que se valide que no contiene información sensitva, se eliminará del monitoreo. | N/A | Ver detalle del cambio |
| **Firewalls** | | | **Validar** | | | |

Fig. 2.13 Bitácora de seguimiento

## Desarrollo en el tiempo

El desarrollo del proyecto se dio en dos fases, mismas que se detallan a continuación en la figura 2.14.

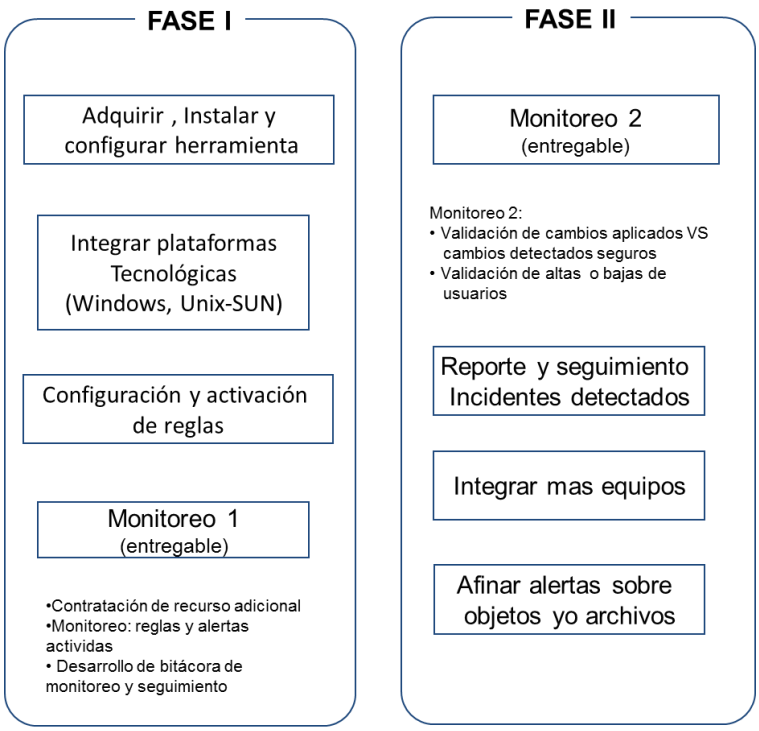



Fig. 2.14 Fases del proyecto

## Resultados

El monitoreo de FIM ha dado satisfacción a la empresa, se logró dar cumplimiento a las revisiones externas y se ha establecido como un requisito de seguridad indispensable, que se debe cumplir en la nueva infraestructura adquirida desde el año 2009. Hasta la fecha continúa en funcionamiento y el proceso de monitoreo ha pasado por diversas fases de mejora, dando mejores resultados. Con este monitoreo se logró impulsar las bases para tener un proceso de respuesta a incidentes.

La empresa ha crecido tanto en la infraestructura como en la plantilla de seguridad dedicada a este proceso. Se contrató personal especializado y dedicado a realizar estas revisiones.

Actualmente se monitorean alrededor de 40 dispositivos tanto de Windows Server como UNIX-SUN y bases de datos SQL Server e Informix.

Como plan de mejora continua se pretende aumentar el número de dispositivos a monitorear.

## 2.3. Escaneo y análisis de parches y vulnerabilidades.

Una de las preocupaciones más importantes para los profesionales en seguridad de la información es el constante aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de los atacantes, la suma de estos dos factores (ataques + vulnerabilidades) pueden ocasionar daños a los sistemas de información y la infraestructura de TI que los soporta.

Lo anterior nos lleva a pensar a inicios del 2009 que se necesita contar con una estrategia cada vez más robusta y efectiva para mitigar este tipo de amenazas. Ciertas empresas realizan un análisis a nivel técnico de las vulnerabilidades de software, asociadas a sus activos de tecnológicos y un análisis de riego que les permita obtener un panorama más claro sobre las amenazas a los que se puede enfrentar una organización.

### Objetivo

Implementar y ejecutar un esquema que garantice la seguridad de la información, estableciendo los procesos necesarios y los mecanismos que garanticen la mitigación de vulnerabilidades en la infraestructura de TI. Llevar a la práctica un plan de escaneo y gestión de parches y vulnerabilidades sobre la infraestructura de TI de acuerdo a los requerimientos de cumplimiento y revisión externa.

### Descripción del proyecto

La gestión de parches de seguridad es un proceso necesario en todas las plataformas; todos los proveedores principales de software que estén comprometidos con la seguridad lanzarán parches de seguridad en respuesta a las nuevas vulnerabilidades identificadas. No hay ningún sistema operativo o aplicación de uso generalizado que sea inmune a los atacantes que dedican su tiempo a intentar localizar vulnerabilidades que aprovechar.

El análisis de vulnerabilidades el cual contempla un proceso de análisis de riesgo sobre las vulnerabilidades, es una actividad que puede orientar hacia un sistema de gestión en seguridad de la información.

El proyecto contemplo dos rubros en fases diferentes :

- Escaneo de servidores productivos (FASE 1). Marzo 2009 - Noviembre 2009
- Escaneo de PCs de la organización (FASE 2). Marzo 2010 - Noviembre 2010

Como primer etapa se considera la implementación de la infraestructura y procedimientos necesarios para ejecutar los escaneos en servidores de producción. El caso de estudio de este proyecto sólo abarca esta primera fase.

## Desarrollo del proyecto

El desarrollo contempló diferentes fases de entendimiento sobre cómo se planeó ejecutar el proceso de escaneo así como las diversas variantes a cubrir.

A continuación se describen las diferentes fases:

- **Entendimiento de la infraestructura de TI.**

Se contempló identificar cada dispositivo hardware residente en la infraestructura de la organización y que soportan los procesos del negocio. Como primer fase se identificaron los equipos que se muestran en la siguiente tabla.

Tabla 2.4 Infraestructura de TI – Escaneos de parches

| Cantidad | Sistema | Plataforma |
|---|---|---|
| 8 | Unix Solaris | Procesamiento Batch |
| 18 | Windows | Red y Producción |
| 2 | AIX | IBM - Ecommerce |
| 28 | | |

- **Pruebas.**

Se clasifican los dispositivos seleccionados, de acuerdo al proceso de negocio que operan y al riesgo. Se evalúa la herramienta a utilizar para la ejecución de escaneo de parches y vulnerabilidades, tras una evaluación técnica y financiera la herramienta adquirida es una de la familia de McAfee, FOUNDSTONE.

- **Medidas preventivas.**

Una vez acotado el universo de pruebas y definida la herramienta para realizar el escaneo, se definen algunas medidas preventivas como las siguientes:

- Horario de pruebas para actividades de escaneos.
- Definir estrategia de contingencia, respaldo de información, respaldo de configuración, entre otros.
- Monitoreo de los servicios durante las pruebas.
- Monitoreo de tráfico de red.

- Informar a operaciones de las pruebas y a los dueños de los activos.
- Informar resultado de las pruebas.

Las pruebas realizadas fueron internas con conocimiento a las áreas involucradas y se estimó un rango de 4 horas para realizar el primer escaneo sobre un universo de 28 equipos.

,

- **Análisis de explotación de vulnerabilidades**

  Las vulnerabilidades descubiertas durante el escaneo se clasifican conforme a la criticidad del fabricante, estas mismas son revisadas y se busca la forma en que la vulnerabilidad puede ser explotada y afectar a los sistemas.

- **Análisis de resultados**

  Con base al análisis de explotación y a la clasificación de la vulnerabilidad se presentan los resultados a la Dirección General, donde se expone los resultados obtenidos. Se asignan tiempos y responsables de las remediaciones.

- **Planes de remediación**

  Los administradores de sistemas en conjunto con seguridad informática generan los planes de remediación para resolver las vulnerabilidades encontradas. Este plan de remediación se realiza con base a clasificación de la vulnerabilidad que se obtiene en la propia herramienta, con finalidad de atender las más críticas.

## Arquitectura y esquema de trabajo

Foundstone fue la solución implementada, después de realizar las evaluaciones técnicas y financieras correspondientes, la herramienta Foundstone fue la mejor calificada según los criterios establecidos por la organización.

Foundstone es una herramienta que cuenta con la plantillas de escaneo avaladas por PCI y la cual contiene los criterios de evaluación para la ejecución de los mismos, esto fue un factor muy importante. Adicional a esto, la herramienta cuenta con la bese actualizada de criterios de evaluación y clasificación de vulnerabilidades de CVE (Common Vulnerabilities and Exposure).

El CVE es un organismo con reconocimiento mundial utilizado por profesionales de la seguridad para obtener información sobre las vulnerabilidades y la criticidad.

A continuación en la figura 2.13 se muestra la arquitectura y esquema implementado.

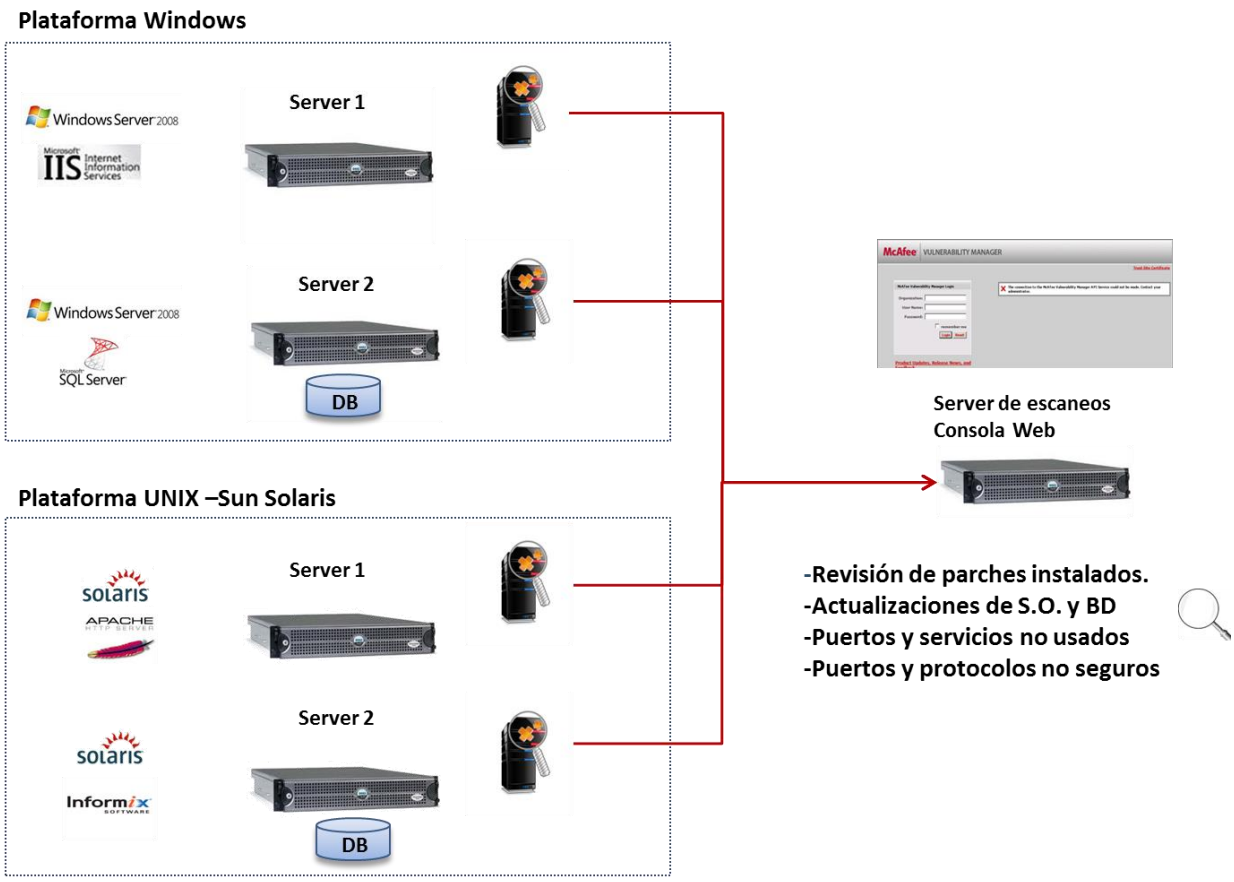



Fig. 2.15 Diagrama conceptual de escaneos

La ejecución de escaneos así como la instalación de parches se estableció con base en un calendario con la finalidad de planificar o proyectar ventanas de mantenimiento que no afectaran a la operación de la organización.

La ejecución del calendario es trimestral y logra cumplir con la norma PCI. A continuación en la figura 2.16 se muestra un ejemplo del calendario.

| SERVIDORES SOLARIS SUN PRODUCCION | | | | | | | Estatus | Primer Escaneo Calendario de Escaneos 27-ene-11 | 28-ene-11 | 03-feb-11 | 04-feb-11 | 10-feb-11 | 11-feb-11 | 17-feb-11 | 18-feb-11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | [redacted] | [redacted] | NA | Respaldo Servidor para Web File Transfer | Solaris 10 | | X | | | | | | | |
| | 2 | [redacted] | [redacted] | NA | Respaldo DMZ Web Server Bancomer | Solaris 10 | Pendiente, se trasladara a Pachuca, F/S | | | | | | | | |
| | 3 | [redacted] | [redacted] | NA | CIC , Vida Bancomer, Vida Bancomer y Aplinet | Solaris 10 | | X | | | | | | | |
| | 4 | [redacted] | [redacted] | NA | DMZ WebServer Banamex | Solaris 10 | | | | | | | | X | |
| | 5 | [redacted] | [redacted] | NA | Connect Direct | Solaris 10 | | X | | | | | | | |
| | 6 | [redacted] | [redacted] | NA | Batch Intercambio | Solaris 10 | | X | | | | | | | |
| | 7 | [redacted] | [redacted] | NA | Conexiones para Aeroméxico | Solaris 10 | | | | | | | | X | |
| | 8 | [redacted] | [redacted] | NA | Application Server Bancomer | Solaris 10 | | | | X | | | | | |
| | 9 | [redacted] | [redacted] | NA | Respaldo Connect Direct | Solaris 10 | | | | X | | | | | |
| | 10 | [redacted] | [redacted] | N/A | Servidor WEB Bancomer | Solaris 10 | | | | X | | | | | |
| | 11 | [redacted] | [redacted] | N/A | DatosSecureTransport | Solaris 10 | | | | X | | | | | |
| | 12 | [redacted] | [redacted] | N/A | Captura manual y captura electrónica | Solaris 10 | | | | | | X | | | |
| | 13 | [redacted] | [redacted] | N/A | Respaldo Batch | Solaris 10 | | | | | | X | | | |
| | 14 | [redacted] | [redacted] | N/A | Application Server Banamex | Solaris 10 | | | | | | X | | | |
| | 15 | [redacted] | [redacted] | N/A | DMZ WebServer Bancomer | Solaris 10 | | | | | | X | | | |

Fig. 2.16 Calendario de escaneos

De la misma forma se estableció una matriz de seguimiento sobre el escaneo de los equipos y cierre de vulnerabilidades, en la figura 2.17 se puede observar un ejemplo del seguimiento.

E-GLOBAL

RESULTADOS ESCANEO DE PARCHES Y VULNERABILIDADES

| DATOS | | | PARCHES Y VULNERABILIDADES | | | | | |
|---|---|---|---|---|---|---|---|---|
| IP | Servidor | Fecha | High | Medium | Low | Pricipales causas | Acciones a realizar | Fecha compromiso |
| [redacted] | [redacted] | 06-may-09 | 0 | 9 | 2 | Actualizaciones de Iexplorer.<br>Parche o actualizacion de IBM Tivoli.<br>Parches y/o actualizaciones de Intel LAN Driver. | Ventana de mantenimineto para instalacion de actualizaciones | Por confirmar |
| [redacted] | [redacted] | 15-abr-09 | 0 | 6 | 4 | Cuenta FTP anonymous Accesible.<br>Aplicación FreeFTP<br>Actualizaciones de Iexplorer | Deshabilitar FTP | Por confirmar |

Fig. 2.17 Seguimiento a escaneos

### Resultados

El proceso ha generado satisfacción a la empresa, se logró dar cumplimiento a las revisiones externas y se estableció como un requisito de seguridad indispensable que los servidores deben ser escaneados y remediados antes de entrar en operación.

En el año del 2010 el proceso de escaneo de parches y vulnerabilidades se extendió para las PC´s utilizando NESSUS como la herramienta de escaneos para PC's.

En el año 2012 como parte de una mejora continua, se optó por realizar una sustitución tecnológica, reemplazando la herramienta FOUNDSTONE por RETINA VULNERABILITY SCAN, esta decisión obedeció al incremento en el número de servidores y en consecuencia de los escaneos. El escaneo se continúa ejecutando con una periodicidad trimestral.

Para el año 2015 se contempla fortalecer la política con la finalidad de establecer un proceso de evaluación y criticidad de la vulnerabilidad de acuerdo a un análisis de riegos e impacto en los servicios en operación.

## 2.4. Programa de capacitación y concientización en seguridad de la información

Sin duda uno de los temas más preocupantes cuando se hace referencia a la Seguridad, es la Capacitación y concientización (Security Awarnes), o mejor dicho la falta de ella. Esto se debe en gran medida a que el usuario en general no es consciente de la importancia de la información que maneja a diario, lo que puede hacer con ella, la utilidad que le puede dar un tercero y las consecuencias de que ésta llegara estar en poder de algún agente no autorizado para conocerla o manipularla por ejemplo.

- **Capacitar,** se refiere a dar a conocer y educar sobre una tema determinado.
- **Concientizar,** está referido a que el concepto/tema sobre el que se está trabajando, realmente se arraigue e incluso llegue a ser un sentimiento en la persona. Muchas veces también se utiliza el término "evangelizar" para reflejar este concepto.

### Objetivo

En el año 2009 para E-Global surgió la necesidad de llevar a cabo la ejecución de un programa de capacitación y concientización que lograra comunicar y sensibilizar a todo el personal sobre la importancia de mantener en la medida de lo posible una operación razonablemente segura.

Implementar la infraestructura y mecanismos necesarios que logren la ejecución y difusión de un programa de capacitación y concientización en temas de seguridad.

## Descripción del proyecto

La seguridad trabaja en conjunto en tres grandes niveles; gente, procesos y tecnología.

Las organizaciones cuentan con controles basados en tecnología, estos controles son operados por gente/personas bajo un procedimiento o proceso.
(Véase figura 2.18).

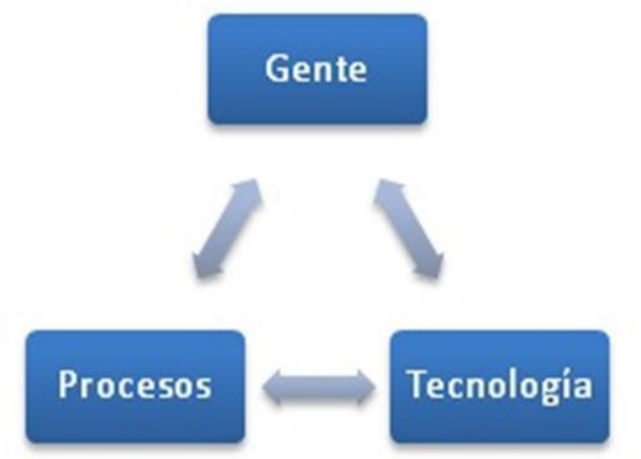



Fig. 2.18 Interacciones esquema de seguridad

El esfuerzo de este programa de capacitación y concientización en seguridad de la información o "Security Awareness" (término en inglés) está enfocado a fomentar entre las personas/gente una conciencia en aspectos o temas de seguridad de la información, el propósito de este programa es tratar de reducir la brecha de desconocimiento y sensibilizar a la organización sobre los diferentes tipos de ataques, prácticas o métodos que se realizan y a los que las personas son vulnerables, con la única finalidad de obtener información de una empresa o persona.

Un programa de capacitación y concientización ayuda a establecer un vínculo entre los profesionales de la seguridad y el personal de la empresa. Dentro del argot de la seguridad se menciona siempre que el eslabón más débil son las personas. Con frecuencia se menciona que aunque una organización tenga implementado los controles de seguridad más estrictos y rigurosos si al personal no se le capacita y concientiza sobre la seguridad de la información se tendrá una brecha de seguridad abierta, las personas son quienes tienen acceso a la información y manejan la misma, y como tal tienen la capacidad de divulgar en cualquier medio ya sea en forma verbal, impresa o lógica.

Bajo esta premisa se trabaja y construye un programa de capacitación y concientización que logre sensibilizar al personal de la empresa y se reduzca el riesgo de cometer una desviación o incidente a las políticas de seguridad de la organización y garantice en la medida de lo posible la confidencialidad, integridad y disponibilidad de la información.

El programa no sólo involucra a la gente que opera procesos o tecnología, sino que abarca desde el guardia de seguridad de la entrada de un edificio hasta el alto directivo. La meta de este programa es involucrar a todo el personal que trabaja en la organización y se logre difundir conceptos básicos sobre seguridad de la información.

El reto es lograr implementar la infraestructura necesaria para difundir temas de seguridad así como una plataforma de e-learning con la cual se pueda otorgar cursos online sobre temas de seguridad de la información.

## Arquitectura del proyecto

La arquitectura utilizada está basada en Open Source. Se utilizaron dos desarrollos, XAMPP y JOOMLA.

- JOOMLA: Es un sistema de gestión de contenido (CMS, por sus siglas en ingles); es un software que permite organizar y facilitar la creación de documentos y otros contenidos vía web dando un forma cooperativa al diseño. Con frecuencia, un CMS es una aplicación web usada para gestionar sitios web y contenidos web. Ayuda a construir sitios web y otras aplicaciones en línea. Joomla! es una solución de código abierto y está disponible libremente para cualquiera que desee utilizarlo.

- XAMPP: Es un software libre, que integra una distribución de Apache completamente gratuita además de contener completamente y de manera gratuita las distribuciones de, base de datos MySQL, y los intérpretes para lenguajes de script: PHP y Perl. El nombre proviene del acrónimo de X (para cualquiera de los diferentes sistemas operativos), Apache, MySQL, PHP, Perl.

Esta soluciones fueron montadas sobre una arquitectura de ambiente virtual basada en la solución del fabricante VmWare bajo su licencia gratuita VmWare Player (véase figura 2.19).

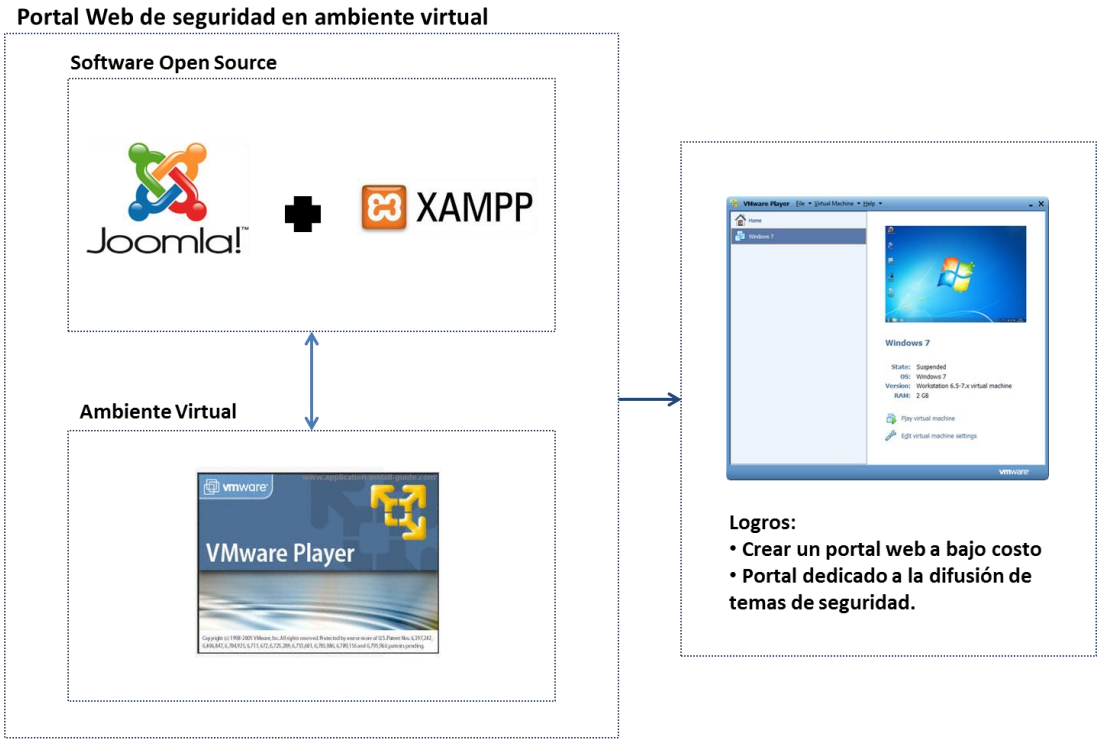



Fig. 2.19 Ambiente virtual portal web

Al conjuntar estas dos soluciones se logró obtener un gestor de contenido web dedicado a la difusión de la Seguridad de la Información, estos primeros temas fueron Phising y Correo Spam (ver figura 2.20)

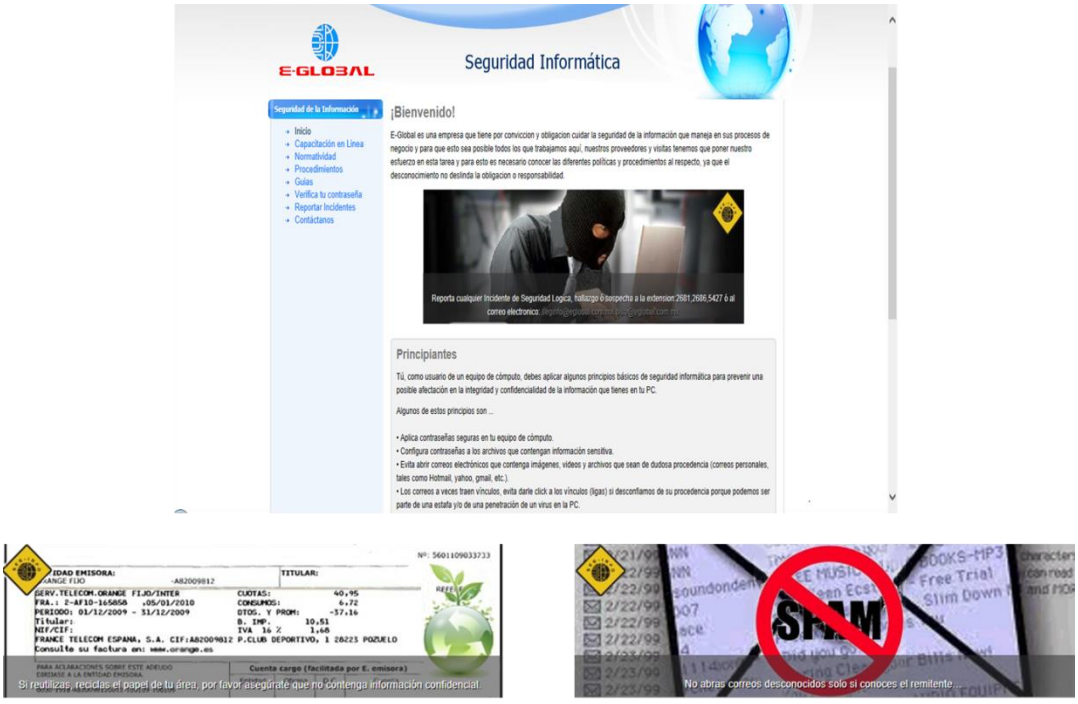



Fig. 2.20 Portal Seguridad de la información

El siguiente paso fue implementar la plataforma E-Learning.

E-learning es la forma de realizar una capacitación o cursos a distancia, utilizando una plataforma electrónica. La implementación de esta plataforma también está basada en arquitectura OPEN SOURCE conocida como CLAROLINE.

Claroline: Es un software de código abierto para implementar fácilmente una plataforma dedicada al aprendizaje y la colaboración en línea de fácil uso (Ver figura 2.21).

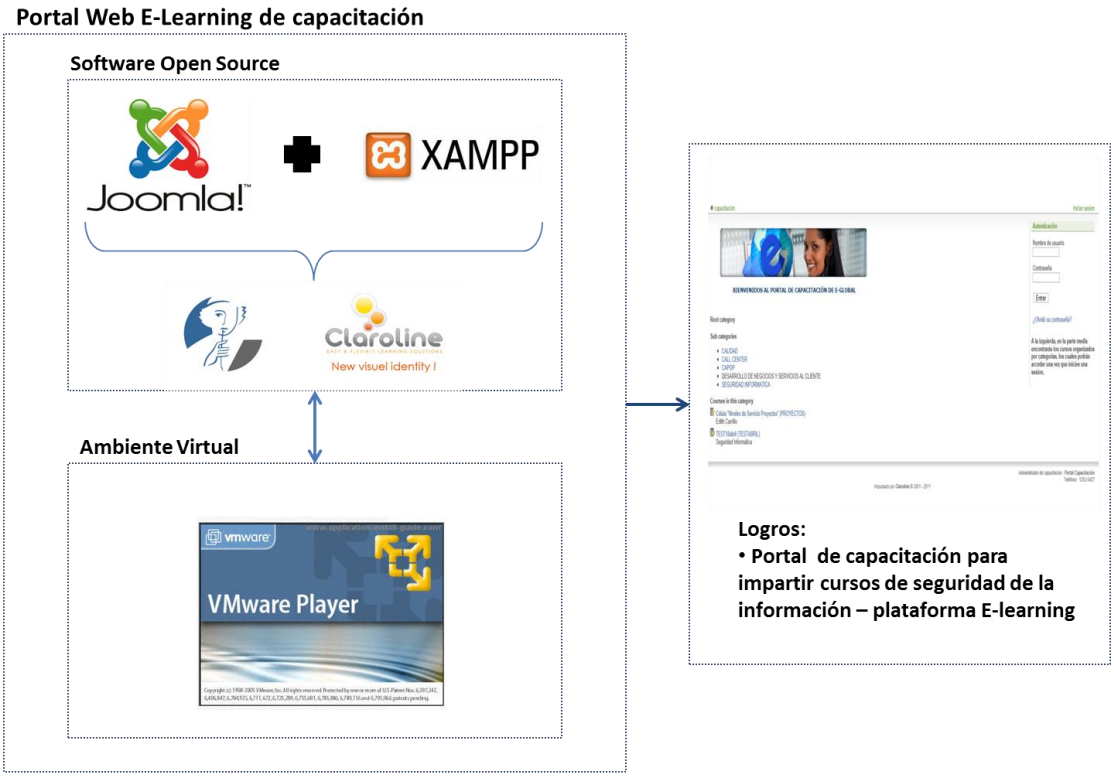



Fig. 2.21 Ambiente virtual - E-Learning

Con esta arquitectura se logra obtener un portal web con la capacidad de administración y realización de cursos de capacitación vía intranet (on-line). Se desarrollaron cursos para promover el uso correcto de las contraseñas, la clasificación de información concientizar sobre temas de spam y el uso correcto de correo electrónico, entre otros (Ver figura 2.22).

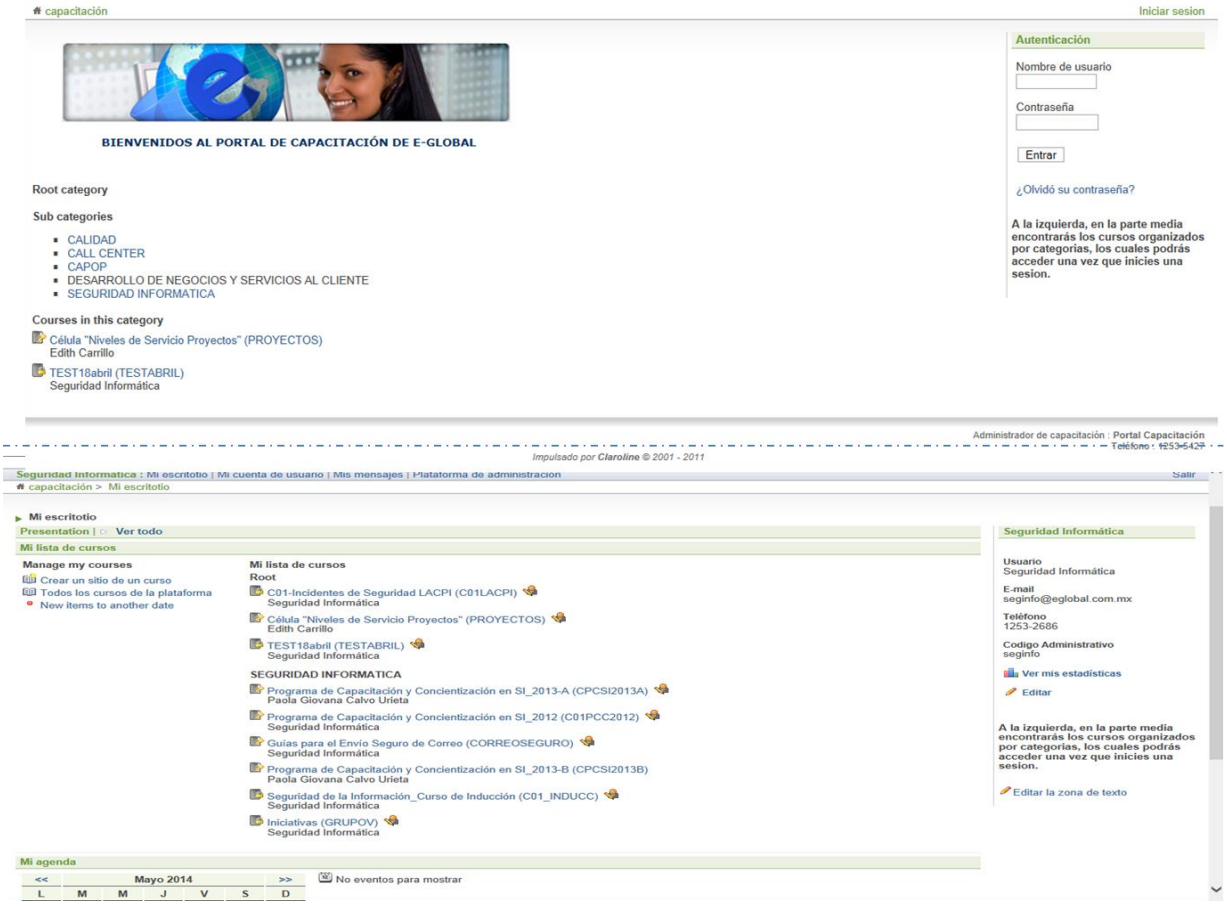



Fig. 2.22 Portal E-learning - Claroline

## Desarrollo en el tiempo

El proyecto consistió de dos fases:

- Implementar la arquitectura y solución.
- Desarrollar el programa de capacitación y concientización de seguridad (programa de Security Awareness, políticas y procedimientos)

A continuación en la figura 2.23 se describen estas fases:

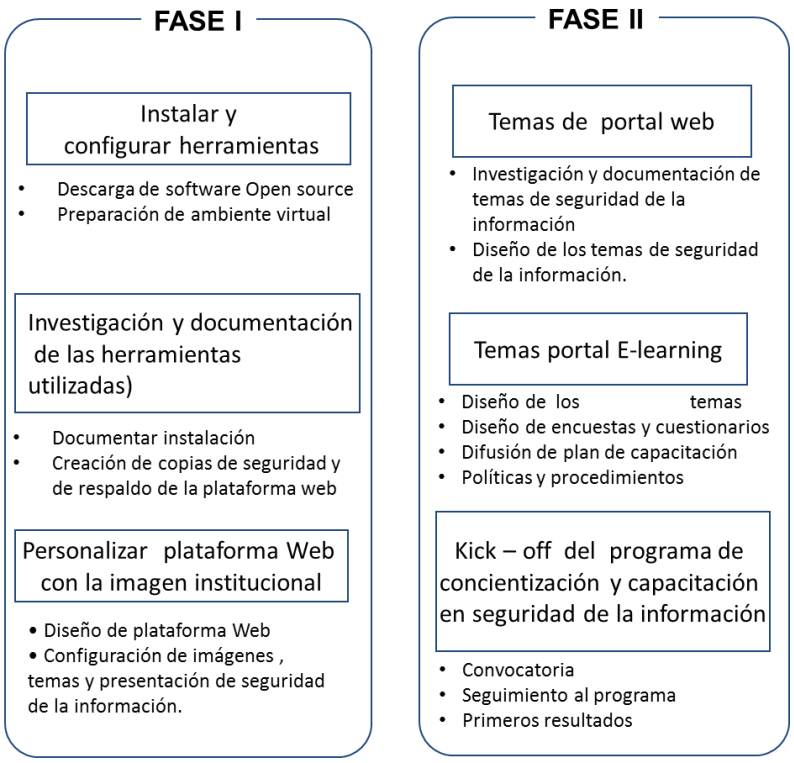



Fig. 2. 23 Fases del proyecto – Plataforma Web

## Resultados

La solución continúa funcionando y es base actual no sólo para impartir cursos de seguridad de la información, también se imparten cursos de otras características, como por ejemplo cursos para capacitar al personal sobre el manejo de dispositivos Terminal punto de venta (TPV), cursos para atender o dar soporte a clientes, encuestas para calificar el desempeño de supervisores, entre otros.

Con respecto a seguridad de la información, con la ayuda de portal se han impartido diversos talleres, en lo que va de este año 2014 se han impartido cuatro talleres de seguridad y dos capacitaciones en conceptos básicos de seguridad superando lo realizado en otros años. Para los siguientes meses de este año 2014 todavía se tiene planeado impartir tres talleres con la ayuda de esta plataforma.

Para el año 2015 se contempla realizar la migración de toda la arquitectura a las nuevas versiones (joomla, vmware, XAMP y Claroline), esto con la finalidad de mantener una plataforma actualizada y con nuevas funcionalidades la cual pueda cumplir con las expectativas de cursos, talleres y capacitación de otros cinco años por lo menos.

# CAPÍTULO 3: Cifrado de transacciones financieras en cajeros automáticos

## 3.1 Antecedentes caso de estudio

La red de cajeros automáticos es uno de los tres pilares de la infraestructura bancaria de cualquier país. Además, es un medio necesario para facilitar a los usuarios del sistema financiero el realizar transacciones financieras de manera más ágil y eficaz. En 1972 ingresó el primer cajero automático en México.

A pesar del incremento creciente de los pagos electrónicos, las operaciones de bajo valor todavía se realizan en efectivo. La mayoría de las operaciones con tarjeta siguen siendo retiros de efectivo en cajeros automáticos. Todos los cajeros automáticos están conectados a través de una red única. La red de cajeros automáticos ha crecido de 2005 a finales de 2009 en un 48% (33,905). El número de cajeros instalados fuera de sucursales en lugares como tiendas de autoservicio, plazas comerciales y tiendas minoristas se incrementó en 62% durante el mismo periodo mientras que el número de cajeros ubicados dentro de sucursales creció en 27%.

La participación de mercado de los cajeros automáticos de los seis bancos más grandes de México bajó de 89% en 2007 a 84% en 2009. En ese mismo año se realizaron más de 1.3 mil millones de retiros de dinero en cajeros automáticos por un valor total de aproximadamente MXN 1.85 billones mientras que en 2005 se efectuaron 1.1 mil millones de retiros de cajeros automáticos con un valor de MXN 1.3 billones. A la fecha de Junio del 2014 se tienen registrados 67870 cajeros en todo el país, las cuales registran un total de 380,969,957 operaciones bancarias (retiros, pagos y transferencias) lo que representa un importe 628,892 millones de pesos.

En México esta red única de cajeros fue creada por Promoción y Operación S.A de C.V (PROSA). Esta red única fue nombrada por PROSA como cajeros compartidos “RED”

La solución de PROSA proporciona enlace, recepción, identificación de destino y enrutamiento de las transacciones generadas por productos aceptados en el Sistema RED: de un cajero automático propiedad del adquirente hacia el emisor de la tarjeta con la que se realiza la transacción.

El Sistema RED interconecta a todas las instituciones financieras del país y a los procesadores TSYS, FDR, Visa / Plus, MasterCard / Cirrus, UnionPay, ATH y Servibanca.

PROSA interconecta bajo el esquema de cajeros compartidos "RED" a la mayoría de los bancos mexicanos con más de 16 mil cajeros automáticos en todo el país (ver figura 3.1).

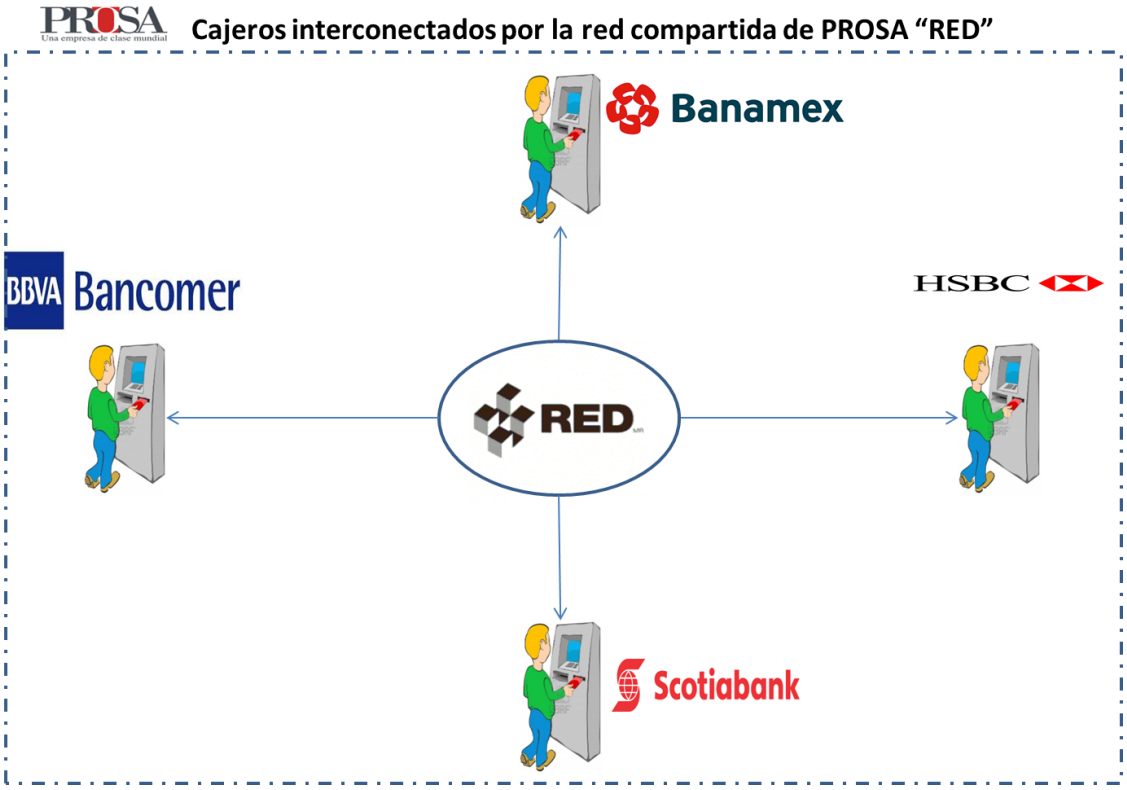



Fig. 3.1 Cajeros "RED" PROSA

## 3.2 Objetivos

EL objetivo principal del proyecto es implementar la infraestructura y mecanismos de cifrado para operaciones transaccionales en la red de cajeros automáticos, la cual debe cumplir con los requerimientos y estándares internacionales que regulan las transacciones bancarias.

El presente trabajo, documenta la estructura y mecanismos de cifrado que se implementaron para llevar a cabo una solución que compita en el mercado actual y el cual pueda interconectar toda una red de cajeros automáticos ATMs y se brinde a los clientes de E-Global como valor agregado en soluciones de medios de pago.

## 3.3 Alcance

La implementación del proyecto por completo está programada en tres fases diferentes, en este trabajo solo se documentan las dos primeras fases y se describen las acciones a seguir correspondientes a la FASE 3, las cuales se enumeran a continuación:

- FASE I - Contempla implementar un ambiente de pruebas utilizando dispositivos Host Security Module (HSM) de cifrado de la marca REALSEC. De igual manera se contempla la generación e intercambio de llaves cifrados en ambiente de pruebas en REALSEC. La prueba de funcionalidad consiste en la pago de servicios (pago de recibo TELMEX, CFE, SKY, entre otros) a través de un cajero automático dentro de las instalaciones de laboratorio. El objetivo de esta fase es empezar a visualizar diferentes escenarios de riesgos y costos que implica el proyecto

  En la figura 3.2 se detallan las actividades relacionadas a la infraestructura de cifrado realizadas en esta fase.

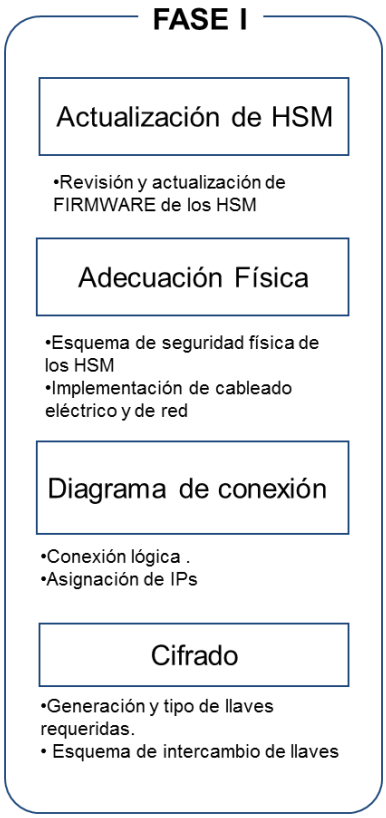



Fig. 3.2 Fase I – Cifrado de cajeros automáticos

- FASE II – Se considera la puesta en producción. Los puntos importantes a considerar, son el cambio de los equipos de cifrado, en esta fase se migrarán de equipos REALSEC a equipos THALES, y una prueba piloto de funcionalidad se realizará en un ambiente contralado con un cajero automático instalado en la recepción del edificio pago de servicios. El propósito de esta fase es tener implementada toda la infraestructura necesaria que pueda soportar la interconexión de cajeros automáticos.

  En la figura 3.3 se describen las actividades de cifrado efectuadas en la fase II.


Fig. 3.3 Fase II – Cifrado de cajeros automáticos

**FASE 3** – Se considera incorporar en el mercado cierto número de cajeros instalados en diversos puntos de la República Mexicana como en plazas, centros comerciales y supermercados. Esta fase hasta hoy todavía está en negociación con el banco cliente para la implementación. Sin embargo se tiene proyectado salir al mercado con la implantación de estos 50 cajeros en el primer trimestre del año 2015.

## 3.4 Introducción

Las nuevas tecnologías de acceso y administración de información han representado una evolución en el concepto de banca, así como los alcances de las instituciones financieras, en términos de nuevos productos y servicios a sus usuarios. Un ejemplo de esta evolución ha sido el desarrollo de las redes de cajeros automáticos. En particular, la ampliación de las redes de cajeros automáticos bancarios ha significado una reducción en algunos costos de transacción para el usuario, así como una mayor capacidad de acceso a liquidez y uso de sus cuentas bancarias en horarios abiertos.

Algunos objetivos de promover y expandir la red de cajeros para las instituciones financieras son permitir una mejor prestación de los servicios financieros e incrementar el número de transacciones de los usuarios existentes.

La operaciones financieras (transaccionalidad) de la red de cajeros, se define como el acceso y uso de una cuenta bancaria a través del sistema de cajeros; en un periodo de tiempo y en función del número de veces que se utiliza el servicio del cajero, el tipo de operación financiera que se realiza (retiro, consulta, depósito u otros) y el monto en efectivo de la operación. Este servicio lo ofrece el propio banco a traves de su infrestructura, o en otros casos, por alguna de las redes de cajeros desarrolladas por otras instituciones (por ejemplo el caso de PROSA con su RED de cajeros compartidos).

Una de las principales preocupaciones de las autoridades financieras es que el acceso a servicios bancarios no se afecte por prácticas de mercado no competitivas de los bancos participantes y, además, que los cobros a los usuarios del sistema sean transparentes. Con lo anterior en mente, en mayo de 2010 el Banco de México modificó su regulación y estableció un cobro único al usuario por parte del dueño del cajero. En particular, el usuario debía pagar la comisión única por acceso a la red a través de la institución donde su cuenta residía. Dicho cambio en la regulación eliminó el cobro que hacían los bancos a sus clientes por usar cajeros ajenos y de facto, también eliminó el cobro de la cuota interbancaria que pagaba el banco del cliente al banco dueño del cajero.

Otra de las principales preocupaciones sobre el uso de los cajeros automáticos son los tipos de fraudes que se pueden realizar.

Las prácticas habituales para llevar a cabo el delito o fraude en cajeros, se pueden catalogar de cuatro maneras distintas según sus características.

- La primera es la trampa de tarjeta, que consiste en la obtención de la tarjeta física original junto al código secreto o PIN, para llevar a cabo este tipo de trampa se cambian los teclados de los cajeros para obtener dicho código y un posterior uso de la tarjeta con los NIP de tarjeta obtenidos.

- Por otro lado también está el Fraude familiar que se caracteriza por el uso ilícito de una tarjeta de crédito por parte de un familiar de la víctima sin el consentimiento de la misma para sacar dinero.

- Otra tercera posibilidad de fraude en los cajeros automáticos que se denomina Clonación de tarjeta y se caracteriza por la obtención del código secreto y los datos de las bandas magnéticas de la tarjeta. Para conseguir estos datos se suele recurrir a dispositivos falsos colocados en el cajero automático.

- Por último se encuentra otro tipo de fraude no tan sofisticado conocido como “trampa del efectivo” que se distingue por la utilización de mecanismos rudimentarios que se colocan en la boquilla dispensadora de billetes del cajero en cuestión con la finalidad de ocultar e impedir que salga el dinero de la víctima. Usualmente los delincuentes que llevan estos delitos a la práctica, no son delincuentes cualesquiera sino que son conocedores y expertos de la práctica, además suele llevarse a cabo entre grupos de delincuentes organizados.

Generalmente, los delincuentes tratan de realizar estas prácticas en cajeros con gran afluencia de personas, en lugares cercanos donde se celebran eventos o festivales o bien en cualquier cajero sobre fechas concretas de cobro. Sin embargo estas prácticas han evolucionado y los intentos por violar un cajero y hackear un cajero han aumentado.

Ataques de virus o malware en el sistema operativo hasta intentos de intrusión para vulnerar el cajero automático y obtener los datos del tarjetahabiente son más frecuentes y las técnicas mejoran día con día.

El objeto de este trabajo es precisamente evaluar, establecer e implementar los mecanismos de seguridad para tratar de mantener la confidencialidad e integridad de los datos de tarjetahabientes, con la única finalidad de que sean protegidos durante todo el ciclo de vida y procesamiento de la transacción.

Para E-Global como institución que brinda servicios financieros de medios de pago, el proyecto de switch de cajeros no es ajeno al cumplimiento de regulaciones nacionales e internacionales. En este caso la entidad que avala el procesamiento de transacciones en cajeros automáticos es VISA el cual ejecuta la evaluación o auditoría del PIN de forma anual. Y como requerimiento internacional para realizar transacciones con otras redes de cajeros es indispensable cumplir los controles y requerimientos de seguridad más altos de la industria.

## 3.5 Marco Teórico

A continuación se describen los antecedentes teóricos y conceptos básicos que permiten el correcto desarrollo del proyecto caso de estudio de este trabajo.

### 3.5.1 Criptografía

#### Terminología y significado

La Criptología (del griego criptos= oculto y logos= tratado, ciencia) es la ciencia que trata las escrituras ocultas, está comprendida por la Criptografía, el Criptoanálisis y la Esteganografía.

Actualmente la criptografía es considera una ciencia, y se define como la ciencia que se encarga del estudio de técnicas para transformar la información a una forma que no pueda entenderse a simple vista; sin embargo, el objetivo de la Criptografía no es sólo mantener los datos secretos, sino también protegerlos contra modificación y comprobar la fuente de los mismos.

El objetivo principal de la criptografía es "ocultar" el mensaje, llamando a este proceso "cifrado", y sólo el receptor con una llave o clave secreta pueda "descifrarlo" y leer su contenido.

En términos generales la criptografía describe las técnicas que permiten cifrar mensajes o hacerlos ininteligibles. El verbo asociado es cifrar.

Cabe mencionar que México ha tenido su historia en el uso de la criptografía, México fue el primer país en el continente americano donde se usó la criptografía. Y sucedió con uno de los hechos más importantes de la historia en el mundo, el pasaje se conoce como el Telegrama Zimmermann. En este telegrama, Alemania propone a México unirse en contra de Estados Unidos para formar una alianza con Japón, a cambio en caso de derrotar a Estados Unidos, regresaría a México los territorios perdidos de Texas, Arizona y Nuevo México.

## 3.5.2 Cifrado

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que disponga de la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra en un sitio web, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse con el fin de mantenerla a salvo.

En la figura 3.4 se ejemplifica un esquema básico de un sistema de cifrado.

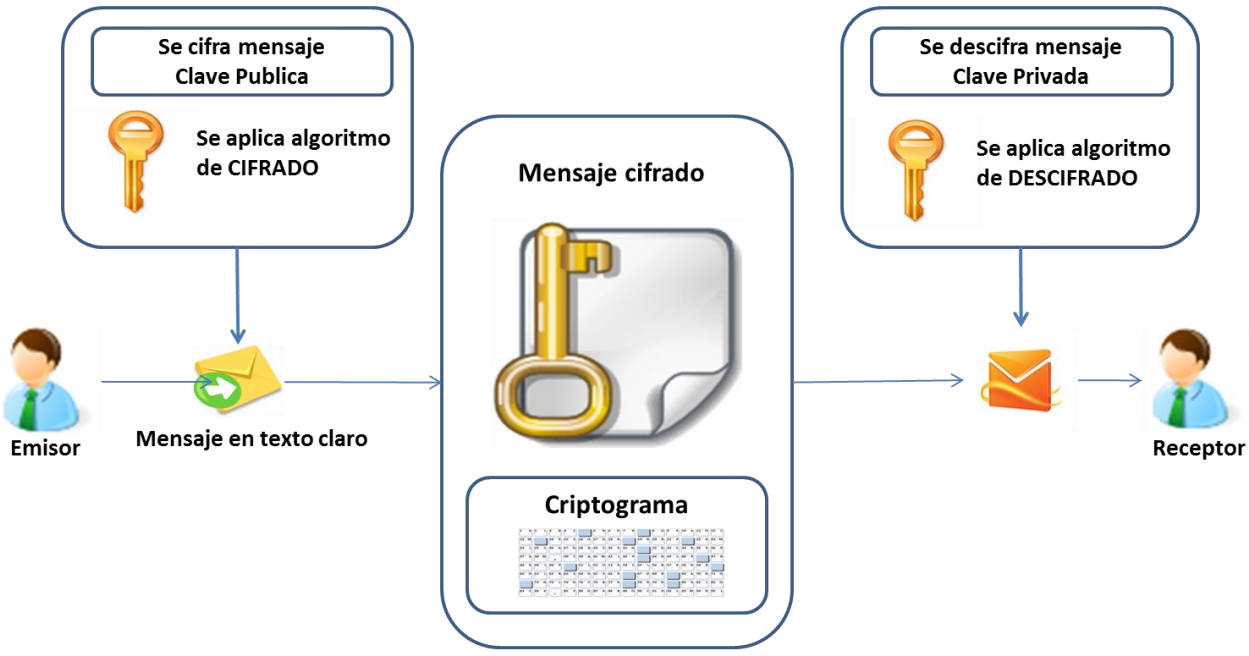



Fig. 3.4 Esquema de cifrado de un mensaje

El emisor envía mensaje original (mensaje en texto claro), mediante un procedimiento utilizando algún algoritmo de cifrado o clave, el mensaje original es cifrado es decir se transforma en un mensaje cifrado (también conocido como criptograma) que se envía por un medio de comunicación (enlace VPN, MPLS, E1, internet, etc). El receptor que conoce la clave, transforma el mensaje cifrado (criptograma) en el texto original con ayuda de un algoritmo de descifrado.

En conclusión se pueden definir los elementos básicos de la criptografía: El mensaje "original", el método de cifrado, la llave de cifrado, el mensaje cifrado, el método de descifrado, la llave de descifrado, y el mensaje descifrado.

La criptografía no surge con la era informática, sino que ya viene desde los principios de la historia quisa desde el 500 A.C. Algunos ejemplos de los algoritmos que han sido utilizados son: rellenos de una sola vez, sustitución, transposición, estos ejemplos son conocidos como algoritmos de criptografía tradicional.

La criptografía moderna se basa en las mismas ideas básicas que la criptografía tradicional, pero con una distinta orientación. Se buscan algoritmos de cifrado más robustos y complicados y se puede clasificar en dos grandes grupos: la criptografía de clave secreta o simétrica y la criptografía de clave pública o asimétrica (véase figura 3.5).

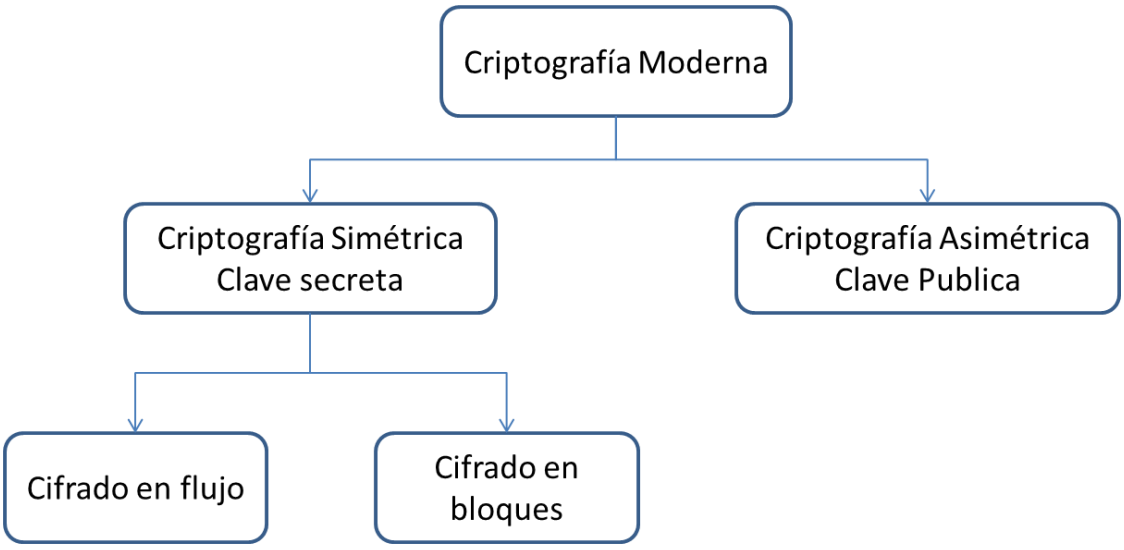



Fig. 3.5 Criptografía moderna

### a) Criptografía Simétrica

También conocida como criptografía de clave secreta es aquella que utilizando algún algoritmo cifra y descifra un mensaje utilizando una única clave secreta.

La clave o llave secreta utilizada es la misma para cifrar y descifrar el mensaje, esto implica que el emisor y receptor del mensaje son los únicos que deben conocer la clave secreta.

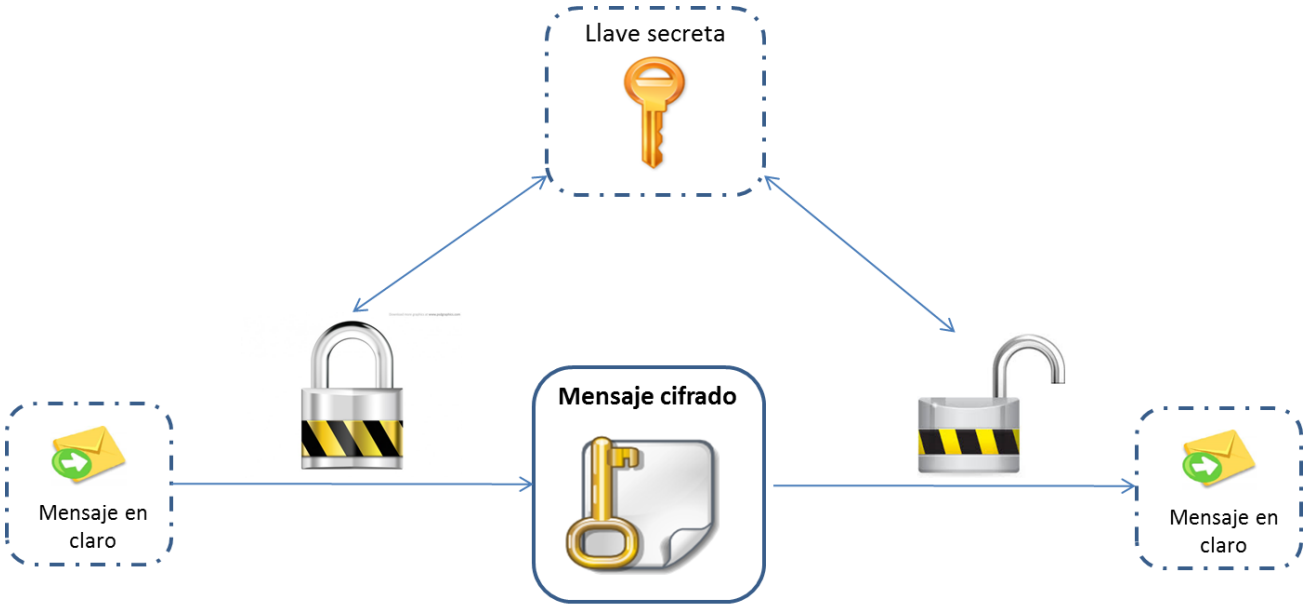



Fig. 3.6 Cifrado simétrico

***Cifrado en Bloques:*** Este tipo de criptografía está basado en el diseño propuesto por Horst Feistel en los años 70. Este método de cifrado opera en grupos o bloques de bits de longitud fija. La longitud de estos bloques varía dependiendo del algoritmo de cifrado, estos algoritmos realizan un cifrado a 64, 96, 128 y 256 bits.

El esquema de funcionamiento general es simple, se divide la información a cifrar en bloques de un mismo tamaño y a cada uno de ellos se le aplican una serie de transformaciones para producir el correspondiente bloque de texto cifrado. (véase figura 3.7)

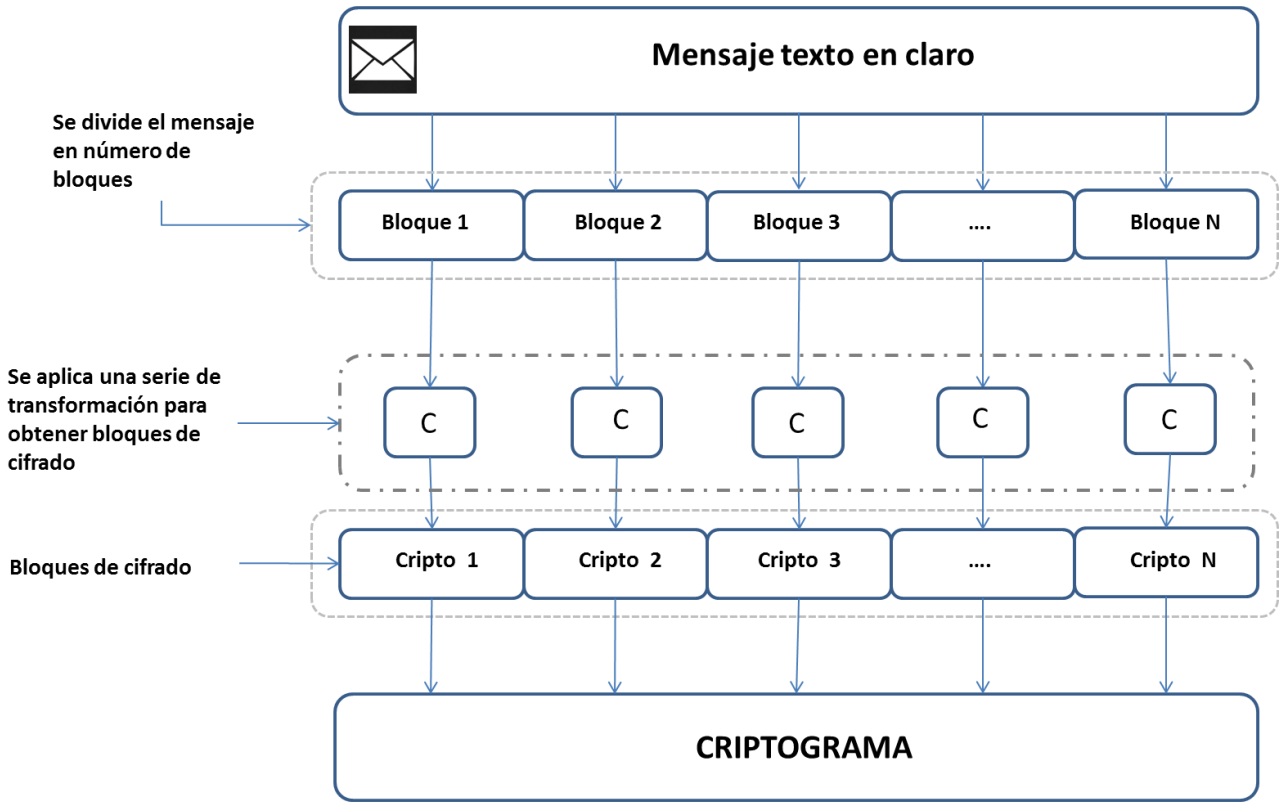



Fig. 3.7 Esquema de cifrado por bloques

Algunos ejemplos de estos algoritmos de cifrado en bloques son:

**DES/3DES:** Data Encryption Estándar fue desarrollado a principio de los años '70 por un grupo de trabajo de IBM. En 1981 la ANSI aprobó el DES como estándar, el X3.92. ISO la aprobó en 1987 con el nombre de DEA-1. Las principales características de este sistema de cifrado es que utiliza operaciones lógicas simples (transposiciones, desplazamientos y XOR's) sobre grupos reducidos de bits (datos de 64 bits), lo que permite una fácil y eficiente implementación del algoritmo en hardware. El problema con este estándar es el tamaño de su llave: 56 bits, para tratar de corregir esto se propuso el triple DES (3DES) el cuál aplica 3 veces el DES, utiliza bloques de 128 bits y claves de hasta 256 bits sustituyen al DES.

**AES:** Advanced Encrition Standard, basado en el algoritmo Rijndael en el año 2001 fue designado como el estándar de cifrado dispuesto por el NIST (National Institute of Standards and Technology), remplazando a al algoritmo DES. AES trabaja con bloques de datos de 128 bits y longitudes de claves de 128, 192, 256 bit según el FIPS 197[34]. Fue elegido como la mejor opción dentro de 15 candidatos. AES es rápido tanto en software como en hardware, es relativamente fácil de implementar, y requiere poca memoria. Como nuevo estándar de cifrado, se está utilizando actualmente a gran escala.

Otros tipos de cifrado en bloques son el RC5 el cual sustituyó al RC4, también existe el RC6 de igual forma que su antecesor el RC5 es un cifrador en bloques. RC6 es muy similar en estructura a RC5 basadas en operaciones XOR.

Existen otros algoritmos de cifrado como es el cifrado en flujo, estos son algoritmos que pueden realizar el cifrado incrementalmente, convirtiendo el texto en claro en texto cifrado bit a bit. Esto se logra utilizando la operación XOR. Se utiliza un algoritmo determinístico que genera una secuencia pseudoaletoria de bits que junto con los bits del mensaje se van cifrando utilizando a operación XOR. Algunos ejemplos de este tipo de criptografía son RC4 (usado en redes inalámbricas), A5/X (usado en telefonía celular, GSM, GPRS).

b) **Criptografía Asimétrica**

También conocida como criptografía de clave pública. Utiliza una clave para cifrar y otra para descifrar. Se usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a la clave privada. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas obtengan casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo. En la siguiente figura 3.8 se ejemplifica el envío de un mensaje utilizando criptografía asimétrica.

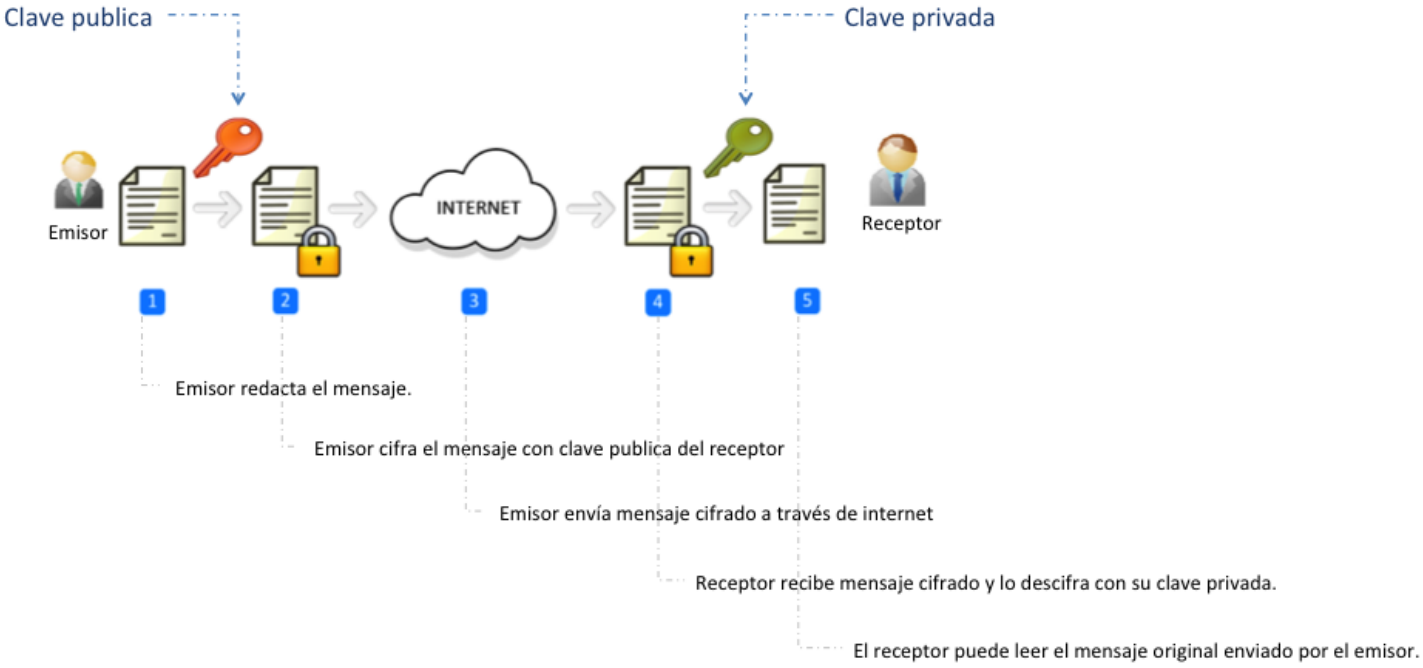



Fig. 3.8 Esquema de cifrado asimétrico

Algunos ejemplos de algoritmos de cifrado asimétrico son; Diffie-Hellma, RSA, ElGamal, Curvas elípticas, Firmas digitales y Funciones HASH.

### 3.5.3 Cifrado por hardware

El cifrado por hardware proporciona una protección más segura frente a los mecanismos de ataques más comunes. Los módulos de seguridad por hardware, denominados Hardware Security Modules (HSM), son dispositivos físicos cuya principal función es el almacenamiento y manejo de llaves criptográficas, además realizan operaciones de cifrado, descifrado y firma digital por medio de algoritmos como AES, 3DES, RSA, DSA, Curvas Elípticas, SHA 1 y 2. Estos dispositivos operan con criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

Por la criticidad de su operación, estos equipos cuentan con certificaciones de seguridad como FIPS 140-2 (Federal Information Processing Standards), Common Criteria EAL 4+ o PCI DSS (Payment Card Industry Data Security Standards), esto asegura que las llaves criptográficas no puedan ser extraídas fuera de los dispositivos y que el almacenamiento y transmisión de datos estén protegidos. En caso de que el equipo fuese abierto, toda la información que almacena se borra.

Estos equipos pueden realizar miles de operaciones criptográficas por segundo y permiten que el manejo de las llaves se lleve a cabo por control dual, bajo autenticación por tarjetas inteligentes, dispositivos USB o contraseñas, además es posible establecer una segregación de responsabilidades (custodios, administradores y operadores). Estos dispositivos son capaces de cifrar cualquier tipo de información (como por ejemplo texto y archivos). Existen modelos similares a servidores (cajas), tarjetas criptográficas que se insertan en la ranura PCI del servidor y otros que se conectan por un puerto USB.

En resumen las principales características que brindan los HSM son las siguientes:

- Suelen implementar procesos criptográficos ampliamente probados y certificados.
- Facilitan la generación, acceso y rotación de múltiples claves de alta calidad.
- Permiten una segregación completa en acceso a las claves criptográficas; de modo que ni los desarrolladores, ni el administrador del servidor de aplicaciones ni el de base de datos puedan ni necesiten tener acceso a las claves.
- Funcionan de tal manera que el código fuente de las aplicaciones que usan los HSM no tengan necesidad de acceder a las claves de cifrado.
- Permiten establecer procedimientos de bajo la “segregación de funciones”, esto permite que nadie pueda disponer de todas las credenciales necesarias para generar o tener acceso a las claves.

- Permiten una trazabilidad de todas las actividades mediante sistemas de auditoría robustos.
- Incorpora mecanismos de seguridad física que dificultan la manipulación de la infraestructura de hardware.
- Posibilitan operaciones de cifrado de alto rendimiento y capacidades de alta disponibilidad.
- Permiten cumplir los requisitos más exigentes de normativas como la PCI/DSS.
- Proporcionan herramientas de desarrollo que permiten integrar funcionalidad propietaria dentro del ámbito de seguridad del propio dispositivo.
- Muchas bases de datos que implementan funcionalidad de cifrado transparente (TDE), pueden ser configuradas para usar las claves almacenadas en HSM.

Otras consideraciones que se deben tener en cuenta, es el eventual costo de los equipos de hardware/software necesarios y su mantenimiento posterior.

En el mercado existen diversas opciones a elegir de acuerdo a las necesidades. Entre los fabricantes más reconocidos a nivel mundial se encuentran Thales, SafeNet, Hewlett Packard, Realsec y Futurex.

### FIPS 140-2

Federal Information Processing Standard (estándares federales de procesamiento de la información), la publicación 140-2, es un estándar de seguridad, desarrollado por el grupo de trabajo del gobierno norteamericano y la industria para validar la calidad de módulos criptográficos. El nombre del estándar es: Security Requirements for Cryptographic Modules (requerimientos de seguridad para módulos criptográficos), que se publicó en 2001 y la última actualización es del 3 de diciembre de 2003.

La serie de publicaciones FIPS 140 para coordinar los requerimientos y estandarización de módulos criptográficos en los que incluye componentes hardware y software. La norma define cuatro niveles de seguridad. La validación FIPS 140-2 especifica el nivel de seguridad al que se ajusta el producto. Existen diferentes niveles de cifrado de acuerdo a los mecanismos de cifrado y protección de los módulos se les asigna un nivel de certificación siendo el Nivel 1 el más básico llegando hasta el nivel 4 como el completo.

Los módulos criptográficos (HSM) tanto los RealSec como los módulos Thales fueron adquiridos con la certificación FIPS 104-2 nivel 3.

### 3.5.4 Cifrado por software

Aunque las aplicaciones de cifrado basadas en software ofrecen cierta protección frente a un acceso no autorizado, son más vulnerables a los ataques. Existen dos aspectos a tener en cuenta a la hora de elegir entre cifrado por software o cifrado por hardware: el rendimiento y la seguridad. Un cifrado por software consumirá recursos (procesamiento, RAM, disco duro, etc. entre otros) al momento de realizar un proceso de cifrado sobre un archivo, base de datos, por ejemplo.

Si un pirata informático consigue vulnerar un cifrado basado en software, es muy probable que pueda manipular los algoritmos para obtener las llaves/claves secretas y pueda facilitar el acceso a la información.

### 3.5.5 Niveles de cifrado

En términos generales la información en los sistemas puede encontrarse en dos estados básicos, en tránsito o almacenados. Tratándose de información sensible, puede ser requerido el cifrado en ambos estados para una protección global de la información a lo largo de todo el ciclo de procesamiento.

#### Datos en Tránsito

El cifrado de la información durante la transmisión evita la pérdida de confidencialidad de la misma. Para el cifrado de la información en tránsito se pueden utilizar protocolos o algoritmos de cifrado, dependiendo de los casos como por ejemplo: IPSec, Https, SSL o ssh, entre otros.

Este tipo de cifrado es utilizado en el desarrollo de este proyecto para cifrar las comunicaciones entre el site de E-Global y los cajeros automáticos.

#### Datos almacenados

Algunas veces el utilizar mecanismos de cifrado en el canal de transmisión no es suficiente, ya que no protege los datos en el origen (antes de la transmisión), ni en el destino, una vez transmitidos.

Por ello, además del canal de transmisión puede ser necesario el cifrado de los datos almacenados (“en reposo”). En este sentido, los datos pueden ser cifrados a diferentes niveles (disco duro, aplicación o base de datos), la siguiente tabla 3.1 muestra las ventajas e inconvenientes de cada uno de estos niveles. Para este proyecto el tipo de cifrado utilizado a nivel de la aplicación, la aplicación es la encargada de invocar las llaves y criptogramas necesarias para realizar los procesos de cifrado y descifrado.

Tabla 3.1 Niveles de cifrado

| Nivel de cifrado | Descripción | Ventajas | Inconvenientes |
|---|---|---|---|
| Sistema Operativo | El cifrado se establece a nivel de disco, volumen o cinta. | Es relativamente fácil de implementar y transparente para el usuario | Efectivo para prevenir el acceso no autorizado a los datos.<br>No ofrece protección nivel del sistema operativo.<br><br>Los backups del sistema operativo requieren de una solución adicional para el cifrado información.<br><br>No cumple con los principales estándares y regulaciones de protección de datos. |
| Aplicación | Todo el proceso de cifrado y descifrado se lleva a cabo por la aplicación. | Se obtiene un mayor grado de protección, el acceso a la información se hace a través del login y a los permisos otorgados<br><br>Sólo se cifran los datos estrictamente necesarios.<br>Simplifica el proceso de backup ya que el dato al estar cifrado en la base de datos (o fichero) se copia cifrado en el soporte de backup.<br><br>Es una buena opciones si es necesario cumplir con regulaciones o estándares de protección de datos. | Al implementar el cifrado a nivel de código fuente puede derivar en vulnerabilidades que comprometan la seguridad al no tener un adecuado manejo de llaves.<br><br>Lo recomendable es hacer uso de librerías de cifrado certificadas que implementen mecanismos robustos y altamente probados (ejemplo: AES 256, 3DES, entre otros) o usar sistemas externos para las funciones criptográficas (ejemplo: uso de HSM o módulo de seguridad hardware) lo cual puede aumentar la complejidad y los costes del proyecto.<br><br>El rendimiento del sistema puede verse afectado si no se hace una implementación adecuada. |
| Base de Datos | Algunos sistemas de bases de datos presentan funcionalidades nativas de cifrado a nivel de campos, datos, tablas, columnas, o la base de datos por completo. Esta funcionalidad suele conocerse como Transparent Database Encryption o TDE<br><br>Se establece un mecanismo de control de acceso que permita que sólo las aplicaciones y administradores autorizados expresamente puedan acceder a los datos. | Presenta un punto intermedio entre las dos opciones anteriores en cuanto a granularidad del control de acceso, sencillez y transparencia de la solución.<br><br>Simplifica el proceso de backup ya que el dato al estar cifrado en la base de datos (o fichero) se copia cifrado en el soporte de backup.<br><br>Es una buena opciones si es necesario cumplir con regulaciones o estándares de protección de datos. | No todos los manejadores de base de datos permiten la funcionalidad de TDE.<br><br>Salvo que la gestión de las claves de cifrado se delegue en un sistema externo (ejemplo: uso de HSM o módulo de seguridad hardware), el administrador de la base de datos podría tener acceso a la información en claro.<br><br>Los datos son descifrados antes de ser enviados a la aplicación, lo cual puede suponer un punto de compromiso de seguridad del sistema que debe ser gestionado.<br><br>Dado que la clave de descifrado debe estar en algún momento en la base de datos (donde los datos cifrados residen), el compromiso de la base de datos puede suponer la pérdida de confidencialidad de los datos al mismo tiempo. |

### 3.5.6 Gestión de llaves y elementos criptográficos

El área de seguridad de la información es la responsable de establecer y documentar los requerimientos y controles necesarios que se deben de implementar para el manejo y gestión de llaves y elementos criptográficos.

Estos controles establecen los lineamientos que se deben seguir y cumplir cuando se realiza alguna actividad en las llaves de cifrado, estas actividades inclyen, generacion, carga, eliminación, de igual manera se establece a los responsables o custodios autorizados por la empresa para desempeñar estas funciones.

A continuación se mencionan de manera general y breve estos controles establecidos para el manejo de los datos de tarjetahabientes:

Todos los procesos y procedimientos de gestión de llaves y elementos criptográficos que se utilizan para el cifrado de datos de tarjetas bancarias y de tarjetahabientes deben estar documentados teniendo en cuenta lo siguiente:

- Generación de llaves robustas (TDES,AES 256, por ejemplo).
- Distribución segura de llaves (en forma de componentes).

    i. Utilizar control dual o conocimiento divido
    ii. Prácticas y métodos de distribución seguros.

- Almacenamiento seguro de las llaves (en dispositivos seguros como HSM).
- Cambios periódicos de llaves.
- Destrucción o remplazo de llaves criptografías antiguas o en sospecha de compromiso.
- Resguardo de llaves de y elementos criptógrafos (uso de caja fuerte, controles físicos de acceso, bitácoras de acceso).

### 3.5.7 Cajeros Automáticos y transacciones financieras

Las nuevas tecnologías de acceso y administración de la información han representado una evolución en el concepto de banca, así como los alcances de las instituciones financieras, en términos de nuevos productos y servicios a sus usuarios.

Un ejemplo de esta evolución han sido el desarrollo de las redes de cajeros automáticos en particular, la ampliación de las redes de cajeros automáticos bancarios ha significado reducción en los costos de transacciones financieras para los usuarios, así como una mayor capacidad de liquidez y uso de cuentas bancarias en horarios abiertos.

Algunos objetivos de promover y expandir la red de cajeros para las instituciones financieras son permitir una mejor prestación de los servicios financieros e incrementar el número de transacciones realizadas por los usuarios.

La transaccionalidad de la red de cajeros se define como el acceso y uso de una cuenta bancaria pasiva a través del sistema de cajeros; y puede catalogarse para un periodo determinado en función del número de veces que se utiliza el servicio del cajero, el tipo de operación financiera que se realiza (retiro, consulta, deposito, por ejemplo), y el número de las operaciones realizadas. Estas transacciones pueden efectuarse en cajeros de la red desarrollada por el banco del usuario (es decir uso de cajeros propios), o en otros casos, por alguna de las redes de cajeros de otros bancos o por alguna red e servicios d medios de pagos como lo es en México el caso de E-Global y PROSA.

En México la entidad y autoridad financiera que regula estas operaciones financieras es Banco de México (BANXICO) y una de las preocupaciones de la autoridad es que el acceso a los servicios bancarios no se afecte por prácticas del mercado no competitivas de los bancos participantes, y además, que los cobros a los usuarios del sistema sean transparentes.

Con este fin Banco de México establece las políticas de cobro y comisiones que deriva en cada transacción realizada en un cajero, se definen en tres tipos de tarifas:

1) Tarifa de cuota interbancaria: esta tarifa, equivalente a la cuota de interconexión (interchange fee), era pagada por el banco emisor al banco dueño del cajero en cada transacción realizada.

2) Cuota de “fidelidad”: esta cuota la cobraba el banco emisor de la tarjeta a su cliente por utilizar un cajero ajeno. Dicha cuota podía ser cero o incluso negativa, dependiendo si el banco emisor cobraba el importe de la cuota interbancaria o daba a su usuario retiros sin costo en cajeros ajenos.

3) Surcharge: En este caso, el dueño del cajero tenía la alternativa de cobrar una tarifa adicional a la de intercambio al cliente usuario. Esta alternativa, era únicamente empleada por un banco en toda su red en México. Dado que la cuota interbancaria es igual entre todos los bancos, se permitía una serie de arreglos en los que las cuotas entre transacciones, bancos y usuarios eran muy distintas. Por ejemplo, algunos bancos emisores permitían un número limitado (tradicionalmente 3) de retiros en cajeros ajenos y cubrían este costo por sus clientes. Otra práctica común era cobrar al usuario propio cuotas superiores a las tarifas de intercambio, generando un beneficio de dicha operación. Dado que la cuota interbancaria es igual entre todos los bancos, se permitía una serie de arreglos en los que las cuotas entre transacciones, bancos y usuarios eran muy distintas. Por ejemplo, algunos bancos emisores permitían un número limitado (tradicionalmente 3) de retiros en cajeros ajenos y cubrían este costo por sus clientes. Otra práctica común era cobrar al usuario propio cuotas superiores a las tarifas de intercambio, generando un beneficio de dicha operación.

Banco de México decide eliminar los esquemas de cobro de tarifas y sustituirlos por una tarifa única que el banco dueño del cajero cobraría al usuario. Esta tarifa única se conoció en el medio bancario nacional como surcharge.

Tal y como se muestra en la figura 3.9, el mercado de ATM se distribuye principalmente entre cinco bancos: BBVA Bancomer, Santander, HSBC, Banamex y Banorte.

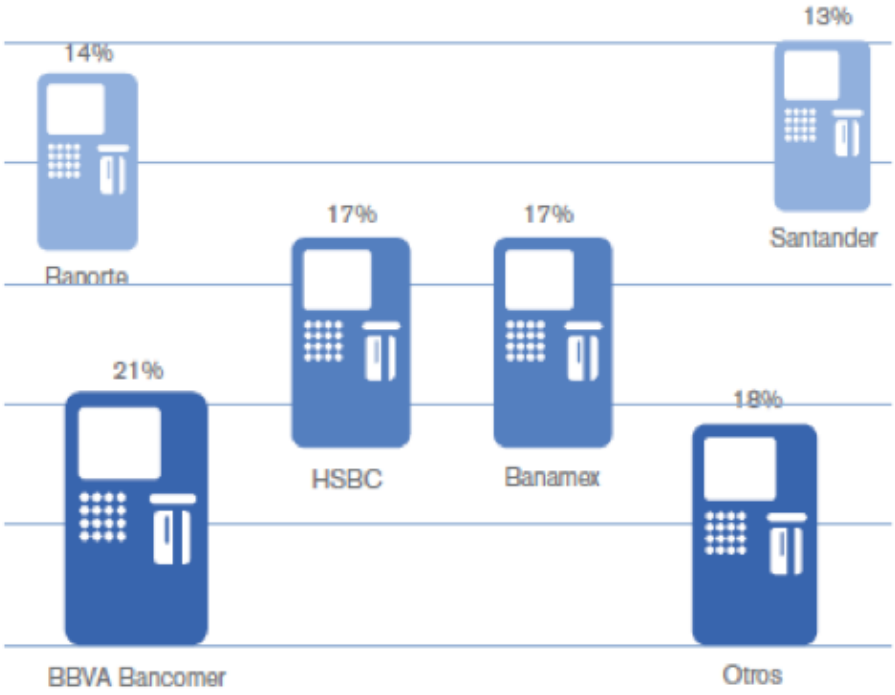



**Figura 3.9 Participación de mercado en ATM**

La función básica de las redes de cajeros (ATM, por sus siglas en inglés) es la de establecer una señal eléctrica que permita transmitir información de los cajeros hacia las cuentas de los usuarios y viceversa, de tal manera que las transacciones en los ATM estén respaldadas por las cuentas bancarias de los usuarios en la institución bancaria donde residen.

Como parte de la apertura en el sector de medios pagos E-Global considera un nicho de mercado importante para ingresar a competir. Es por eso que en enero del 2013 se empieza a vislumbrar la estrategia para incursionar en este sector y en agosto del 2013 se promueve la incitativa para incursionar en los medios de pagos a través de cajeros automáticos, en ese mismo mes se revisan los requerimiento a nivel de la infraestructura necesaria para crear una prueba de concepto y lograr mostrar a clientes futuros potenciales la oportunidad de ofrecerles el servicio y como un valor agregado de E-Global.

### Cajeros automáticos

Los cajeros automáticos, originalmente llamados ATM (Automatic Teller Machine o Máquina de cajero Automático) son dispositivos electrónicos automatizados que permiten a los clientes de un banco hacer la entrega de dinero en efectivo, consultas de saldos y algunas operaciones sobre los diferentes servicios que ofrece una institución bancaria, entregando al usuario un comprobante de la operación en un mínimo de tiempo. Gracias a un cajero automático se pueden utilizar algunos de los servicios que ofrecen los bancos, pero sin tener

que visitar la sucursal. Un cajero automático está disponible las 24 horas del día, los 365 días del año.

Los servicios que éstos ofrecen varían, pero los comúnmente utilizados son:

1. Retiro de efectivo
2. Consulta de saldos
3. Consulta de movimientos
4. Depósitos
5. Pago de tarjeta de crédito
6. Transferencia de fondos

### Cómo funcionan los cajeros automáticos

Sólo se inserta la tarjeta de crédito, débito (los más comunes), se digita una clave personal conocida como NIP (Número de Identificación Personal) y se siguen las sencillas instrucciones que aparecen en la pantalla y que llevan al usuario de la mano para realizar las operaciones que desea.

Existe un sistema de RED de cajeros automáticos a nivel nacional, que ofrece la posibilidad de utilizar cualquiera de ellos, independientemente del banco donde se tenga la cuenta bancaria. Casi todos los bancos están afiliados a este sistema de RED, algunos de ellos le permiten disponer de dinero en toda la República Mexicana y otros a nivel internacional. Como se mencionó anteriormente la propietaria de esta red de cajeros es PROSA y precisamente es denomina RED©.

### Componentes de un cajero automático

Un cajero automático se compone principalmente de:

**Hardware:**

- Un dispositivo para el reconocimiento y validación de billetes.
- Una computadora personal CPU.
- Una pantalla (puede ser un monitor sensible al tacto, llamado touchscreen).
- Lector de banda magnética
- PIN PAD lectora de tarjetas con chip.
- Una impresora de comprobantes.

Su estructura la compone un gabinete exterior de lámina de acero de características y terminado de uso rudo para su instalación en el interior de un edificio o cubículo destinado para este fin. Cuenta con una caja fuerte para el resguardo del efectivo que reciben y del que entregan, a la vez que está protegida con cerraduras de alta seguridad y con llaves únicas.

**Software:**

Hoy en día la gran mayoría de los cajeros automáticos en todo el mundo utilizan un sistema operativo Microsoft Windows, principalmente Windows XP Professional o Windows XP Embedded.

Linux también es utilizado en el mercado de ATM. Un ejemplo de esto es Banrisul, el banco más grande en el sur de Brasil.

Con el paso del tiempo la industria financiera y de medios de pagos a buscado una base de software más estandarizado, sobre todo las instituciones financieras han sido cada vez más interesados en la posibilidad de escoger y elegir los programas de aplicación que impulsan sus equipos. WOSA/XFS, ahora conocido como CEN XFS, proporciona una API común para acceder y manipular los diferentes dispositivos de un cajero automático. J/XFS es una implementación de Java de la API CEN XFS.

### PIN PAD

Es un dispositivo de tipo teclado electrónico utilizado comúnmente en terminales punto de venta o cajeros automáticos, la función principal es poder digitar el PIN (Personal Identification Number). Las PIN pads se usan normalmente con los cajeros automáticos además de permitir la lectura de la banda magnética valida los datos mediante el CHIP inteligente de las tarjetas lo que da un factor más de seguridad además de validar los datos de la tarjeta con el número del PIN, estos datos son cifrados por la pin pd al momento de su captura con el objetivo de mantener la integridad y confidencialidad de los datos. En algunos casos el NIP solo es validado mediante la lectura del CHIP, en este caso el PIN no necesita ser enviado (esto se conoce como "offline verificación del PIN").

Al igual que algunos dispositivos de punto de venta, las PIN pads están equipadas con características de hardware y software de seguridad para asegurar las claves de seguridad inyectadas y el PIN se borran si alguien intenta manipular el dispositivo. El PIN es cifrado inmediato a la entrada y se crea un bloque de PIN cifrado. Este bloque de PIN cifrado se borra tan pronto como ha sido enviado desde el teclado de PIN del dispositivo de punto de venta. Las NIP se cifran utilizando una variedad de esquemas de cifrado, el más común es el triple DES .

Los dispositivos PIN pads deben ser aprobadas por los estándares requeridos en la industria de tarjetas de pago para asegurarse de que proporcionan una seguridad adecuada en el punto de entrada de PIN y para el proceso de cifrado de PIN. ISO 9564 es la norma internacional para la gestión de PIN y de seguridad, y especifica algunos requerimientos y características de los dispositivos de entrada de PIN recomendado.

Aunque los dispositivos PIN pads normalmente permiten la entrada de valores numéricos, algunos PIN pads también tienen letras asignadas a la mayor parte de los dígitos, para permitir el uso de caracteres alfabéticos o una palabra como una regla mnemotécnica para el PIN numérico. No todos los dispositivos PIN pads tienen necesariamente las mismas letras para los mismos números.

En la siguiente figura 3.10 se observan algunos de los distintos tipos de PIN pads que se son utilizados.

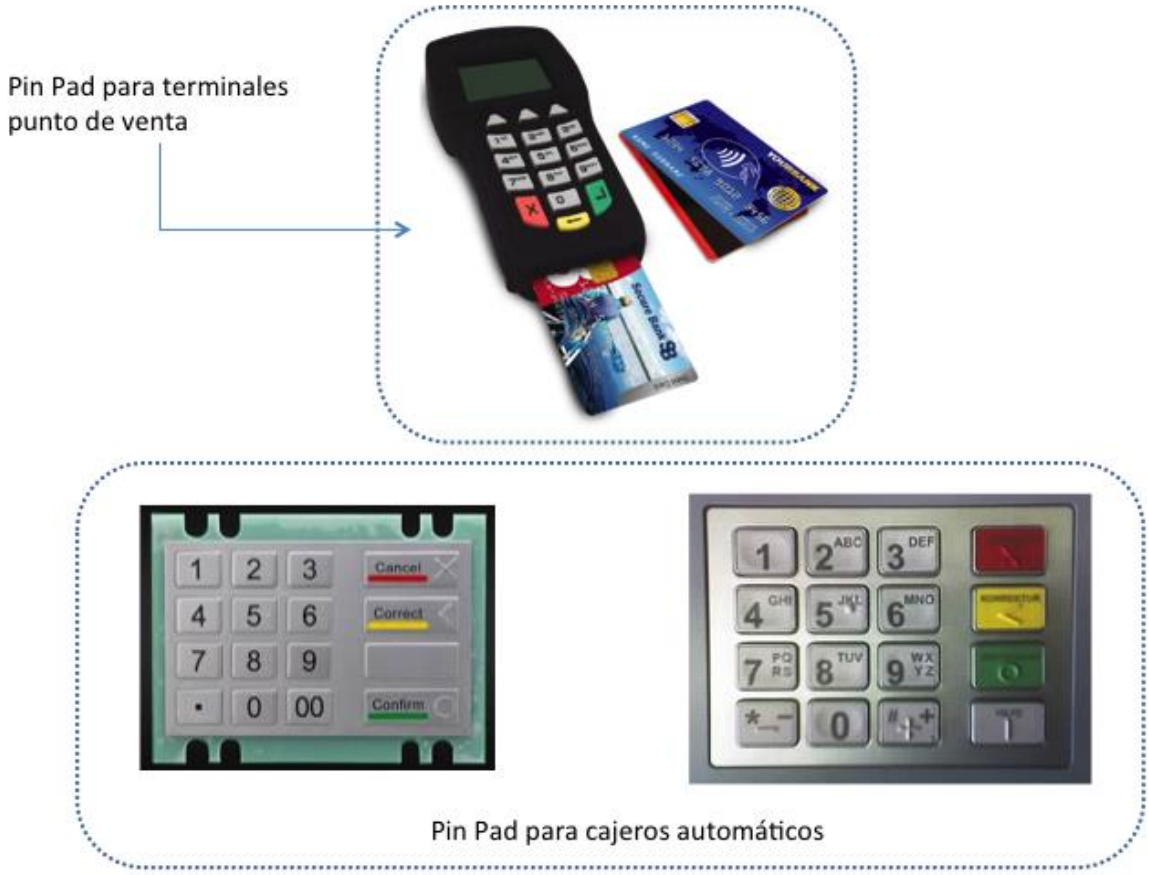



Figura 3.10 Tipos de PIN PAD

## Seguridad en cajeros automáticos

La seguridad que los cajeros automáticos ofrecen a los bancos para el manejo del dinero y de las operaciones que en él se realizan, se da gracias a la alta tecnología que utilizan, contando con sistemas de monitoreo del funcionamiento de cada cajero, sistemas de reporte de fallas, alarma de fallas, sistemas de seguridad remota automática y acceso remoto a los cajeros desde las oficinas centrales del banco, o desde el lugar que se tenga designado para el control y monitoreo de los cajeros automáticos.

La mayoría de los bancos tienen instalados dos tipos de cajeros automáticos:

1. Tipo lobby. Para ubicación en el interior de oficinas o centros comerciales.
2. Tipo empotrable. Para oficinas que pertenecen al propio banco.

**Seguridad Física:** se enfoca en hacer los cajeros automáticos invulnerables a los ataques físicos, son cajas fuertes con mecanismos dispensadores muy bien diseñados para resguardar el dinero. Adicionalmente, existen otros mecanismos de seguridad que se han implementado en los cajeros como por ejemplo el uso de cámaras. Los cajeros automáticos actuales cuentan con cámaras de video que graban las actividades que se realizan.

Estas cámaras generalmente están colocadas en la parte frontal del cajero y una segunda, ubicada dentro del cajero en la parte posterior, la primera cámara (cámara frontal) es activada automáticamente cuando se realiza alguna operación de carga, reabastecimiento de dinero o configuración del cajero, la segunda cámara graba las actividades cuando el cajero es abierto.

Los cajeros cuentan con pantalla anti reflejante con la finalidad de que no se visualice los datos del tarjetahabiente desde ciertas distancias y ángulos de visión.

Algunas características complementarias de seguridad física son las siguientes:

**Sistema de alarmas:** los cajeros automáticos deben estar protegidos por un sistema de alarma adecuado al tipo de cajero y, en lo posible, contar con dos vías de comunicación distintas, de manera que la falla en una de ellas produzca la señal de alarma de la otra. El sistema de alarma y de comunicaciones se debe monitorear permanentemente por medio de una central de monitoreo propia o contratada.

**Circuito cerrado de televisión:** los cajeros deben estar provistos de un circuito cerrado de televisión. Así mismo, es preciso mantener un período apropiado de retención de la grabación. Adicionalmente, el sistema de video debe estar relacionado con la transacción del cliente para garantizar que la imagen sea la correcta (inserción de caracteres en el registro de la operación). Los sistemas de video destinados a la grabación de imágenes deben estar protegidos contra robo y provistos de generadores o reguladores de energía.

**Controles disuasivos:** se deben tener anuncios que adviertan la existencia de componentes de seguridad e incluir medidas preventivas y recomendaciones en la pantalla del cajero, para que los usuarios las tengan presentes al momento de hacer transacciones.

**Visibilidad:** el sitio debe garantizar al cliente la privacidad de su clave secreta. Por ello, la disposición del cajero con respecto a la visualización que tienen las personas desde la parte externa de la cabina no debe facilitar la visibilidad a otras personas cuando se está digitando el NIP.

**Distancia entre cajeros:** en los casos en que existan grupos de cajeros sin cabina (empotrados consecutivamente en la pared o en módulos especiales en centros comerciales), es preciso dejar una distancia prudencial entre ellos (80 cm aprox. de distancia entre cada uno), que permita un grado de confidencialidad en la transacción que un usuario está efectuando.

**Monitoreo físico de los cajeros: l**as entidades financieras deben establecer procedimientos de monitoreo a los cajeros directamente en el sitio, bien sea con personal propio o contratado. La frecuencia de visita debe estar relacionada con el volumen de siniestralidad del cajero y la época del año (fin de año y festividades especiales), haciendo énfasis en visitas aleatorias para evitar que los delincuentes puedan identificar los patrones de visitas.

**Seguridad lógica:** La seguridad de las transacciones ATM se basa principalmente en la integridad del procesador criptográfico. Los métodos de cifrado se usan para prevenir el fraude y garantizar que los datos de tarjeta y tarjetahabiente sean cifrados de inicio a fin, es decir desde que se digitan los datos en la PIN PAD, y se realiza la operación en el cajero hasta que la transacción se ejecuta o procesa.

Como se mencionó anteriormente, el algoritmo estándar utilizado en la industria y avalado por entidades regulatorias nacionales (como por ejemplo Comisión Nacional Bancaria y de Valores CNBV y Banco de México BANXICO) e internacionales (como por ejemplo VISA – Seguridad del PIN), es el cifrado Triple DES (3DES).

Existe una iniciativa para cambiar el tipo de cifrado actual utilizando AES a 256 bits, sin embargo la Industria Financiera a través de entidades que regulan en México como lo son Banco de México (BANXICO) y la Comisión Nacional Bancaria y de Valores (CNVB) aún no estipulan los detalles sobre estos cambios que se deben de aplicar, el Capitulo X de la Circular única de Bancos emitida por la CNBV el 27 de enero del 2010 y en vigor a partir del 28 de julio del 2010 detalla las reglas para la inclusión y operación en la red financiera de México para cualquier institución financiera, este capítulo menciona los métodos y mecanismos de seguridad mínimos requeridos para operar. Muchas instituciones financieras aún continúan con su proceso para migrar llaves de longitud sencilla (DES) a llaves de doble longitud (3DES). E-Global actualmente se encuentra en cumplimiento conforme a los requerimientos de la industria como lo establece VISA, MasterCard, PCI, entre otras.

Por cada POS o ATM tiene que haber una llave maestra (KEK) diferente y debe generarse, al instalar, en forma automática y en línea. Las llaves de trabajo (PIN y MAC) deben generarse automáticamente en el módulo criptográfico (sea por software o hardware) a nivel central y de manera aleatoria (no debe haber intervención manual), estas llaves deben ser cifradas con la llave maestra KEK. Es recomendable que el l intercambio dinámico de llaves se realice con la primera transacción del día.

Además de utilizar los mecanismos de cifrado, los cajeros automáticos cuentan con un CPU con sistema operativo usualmente Windows XP, el cual generalmente corresponde a versiones "recortadas" que no cuentan con todas las funciones de un sistema operativo profesional, estas versiones son limitadas a funciones básicas, así como cambios de configuración, instalación de aplicación, cambios en registros y otras funciones que permitan alterar la integridad del sistema operativo.

### 3.5.8 Tarjetas Bancarias

Las tarjetas bancarias (tarjetas de crédito, débito u otro tipo) son instrumentos utilizados por la banca y sector financiero para la identificación del usuario, regularmente de plástico con una banda magnética, un microchip y un número en relieve. Es emitida por un banco o entidad financiera que autoriza a la persona a cuyo favor es emitida, comúnmente utilizadas como instrumento de medio de pago en los negocios y comercios adheridos al sistema de medios de pago con tarjeta, el pago se efectúa mediante su firma y la exhibición de la tarjeta del titular.

La mayoría de las tarjetas empleadas en el sector financiero consisten en una pieza de plástico, cuyas dimensiones y características generales han adquirido absoluta uniformidad, por uso y las necesidades técnicas. El tamaño de la mayoría de las tarjetas es de 85,60 mm × 53,98 mm en cumplimiento con la norma ISO/IEC 7810 ID-1.

Cada instrumento contiene las identificaciones de la entidad emisora y del afiliado autorizado para emplearla, así como el periodo temporal durante el cual ese instrumento mantendrá su vigencia. Suele contener también la firma del portador legítimo.

Con respecto al origen, se puede decir que apareció en los comienzos del siglo XX alrededor el año 1940 en los Estados Unidos.

Actualmente existen dos tecnologías disponibles para las tarjetas de uso en el sector financiero. La tradicional es la de banda magnética, y las tarjetas con microchip de tecnología más reciente.

#### Tarjetas con banda magnética

Las primeras tarjetas con banda magnética fueron usadas a principios de los años 60s, fueron utilizadas en el transporte público, este evento sucedió en Londres, se instaló un sistema de tarjeta con banda magnética en el sistema de tren subterráneo.

A nivel de entidades financieras las tarjetas con banda magnética se empezaron a usar en 1951. (Ver figura 3.11)


Figura 3.11 Tarjetas plásticas

### Banda Magnética

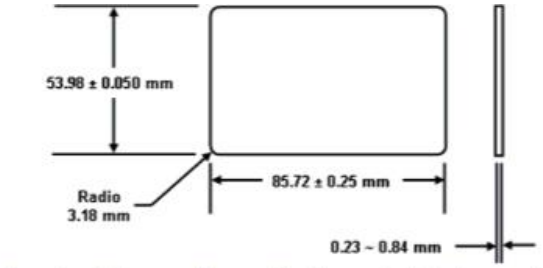
La banda magnética es una banda comúnmente negra o marrón, esta banda está hecha de finas partículas magnéticas en una resina. Las partículas pueden ser aplicadas directamente a la tarjeta o pueden ser hechas en forma de banda y después ser adherida a la tarjeta. Son de baja coercitividad Lo-CO (banda marrón), hecha de óxido de hierro, o de alta coercitividad (intensidad del campo magnético que se debe aplicar a un material para reducir su magnetización) Hi-CO (banda negra) hecha de ferrita de bario. Estos materiales se mezclan con una resina para formar una mezcla espesa que se cubre con un sustrato.

Una vez cubierta con el sustrato las partículas en la mezcla son alineadas para dar una buena señal en proporción al ruido (esto es equivalente a eliminar los estallidos y golpes que se oyen en viejas grabaciones). La banda se pasa con la mezcla espesa aún húmeda a través de un campo magnético para encuadrar todas las partículas.

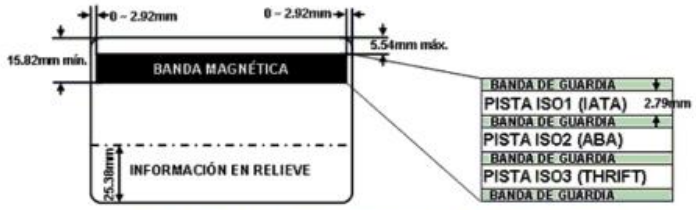
La banda magnética en la tarjeta puede ser codificada porque las partículas pueden ser magnetizadas en dirección sur o norte. Cambiando la dirección de codificación a lo largo de la banda permite escribir la información en la banda. El funcionamiento se basa en la inducción electromagnética, que no es más que un fenómeno que se produce cuando un imán se pasa cerca de un cable, en éste se producirá una corriente eléctrica.

La banda magnética está compuesta por una serie de imanes (dicho a groso modo) puestos en línea, como si se tratase de un código de barras. Al "pasar la tarjeta", estos imanes pasan cerca de un lector, que hace el funcionamiento del cable explicado anteriormente, creando unas corrientes eléctricas pequeñas en función de la distancia entre esos pequeños imanes colocados en la banda magnética, por este motivo, cuando alguien realiza algún pago, la persona encargada de cobrar tiene que pasar la tarjeta por el lector, y cuando lo hacen, tienen que pasarla con cierta velocidad, esto se debe al fenómeno de la inducción magnética. El estándar ISO/IEC 7813 establece los requerimientos de banda magnética para las tarjetas bancarias.

En la figura 3.12 se muestran algunos de los requerimientos específicos para las tarjetas bancarias en cuestión de tamaños y características de banda magnética. Adicionalmente se pueden apreciar las pistas comúnmente conocidas como track´s que componen la banda magnética.




Características en dimensión de una tarjeta bancaria




Características en dimensión de banda magnética

Figura 3.12 Características tarjeta bancaria ISO/IEC 7813

La banda magnética está constituida por tres track´s, en la tabla 3.2 se observan las características de composición de cada track.

Tabla 3.2 Descripción de track´s banda magnética

| Núm. Track | Densidad de grabación (bit x pulgada) | Configuración de caracteres (bit x carácter) | Información de contenido numero de caracteres alfanuméricos |
|---|---|---|---|
| 1 | 210 | 7 | 79 |
| 2 | 75 | 5 | 40 |
| 3 | 210 | 5 | 107 |

En términos generales los tracks de las tarjetas contienen la información necesaria de la cuenta y del tarjetahabiente para poder procesar una transacción financiera. Es por este motivo que al clonar o duplicar una tarjeta bancaria se puede efectuar una operación o transacción financiera sin estar presente el tarjetahabiente. A continuación en las tablas 3.3, 3.4 y 3..5 se describe el contenido y composición de los tracks 1, 2 y 3.

**Tabla 3.3 Composición track 1**

| | **79 <caracteres alfanuméricos>** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CI | CF | PAN | CS | Nombre | Add Data | Diss Data | CF | LRC |

| | Descripción | No. de caracteres | Valor |
|---|---|---|---|
| CI | Centinela inicial | 1 | 05h |
| CF | Código de formato | 1 | |
| PAN | Número de cuenta principal | 19 | |
| CS | Campo separador | 1 | 3Eh |
| Nombre | Nombre | 26 max. | 3Eh |
| Add Data | Fecha de vencimiento | 4 | |
| | Código de servicio | 3 | |
| Diss Data | Datos discretos PVKI* | 1 | |
| | Y/o PVV o offset | 4 | |
| | Y/o CVV* o CVC* | 3 | |
| CF | Centinela final | 1 | 1Fh |
| LRC | Carácter de verificación de redundancia longitudinal | | |

PVKI – Pin indicador de verificación de llave.
PVV - Pin verificador de valor.
CVV – Valor de verificación de tarjeta.
CVC – Código de validación de tarjeta.

**Tabla 3.4 Composición track 2**

| | **40 <caracteres alfanuméricos>** | | | | | |
|---|---|---|---|---|---|---|
| CI | PAN | CS | Add Data | Diss Data | CF | LRC |

| | Descripción | No. de caracteres | Valor |
|---|---|---|---|
| CI | Centinela inicial | 1 | oBh |
| PAN | Número de cuenta principal | 19 | |
| CS | Campo separador | 1 | oDh |
| Add Data | Fecha de vencimiento | 4 | |
| | Código de servicio | 3 | |
| Diss Data | Datos discretos PVKI* | 1 | |
| | Y/o PVV o offset | 4 | |
| | Y/o CVV* o CVC* | 3 | |

| | | | |
|---|---|---|---|
| CF | Centinela final | 1 | oFh |
| LRC | Carácter de verificación de redundancia longitudinal | | |

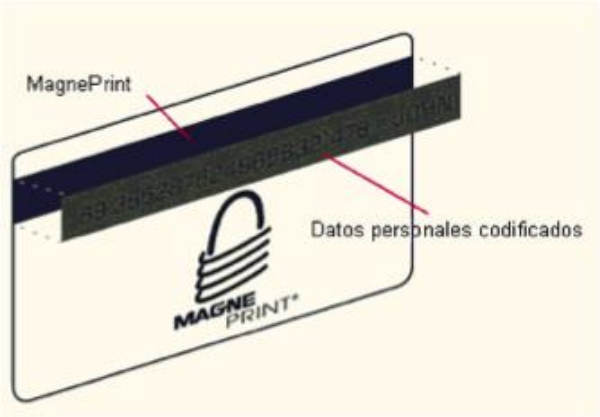
Tabla 3.5 Composición track 3

| | 79 <caracteres alfanuméricos> | | | | | | |
|---|---|---|---|---|---|---|---|
| CI | CF | PAN | CS | Add Data | Diss Data | CF | LRC |

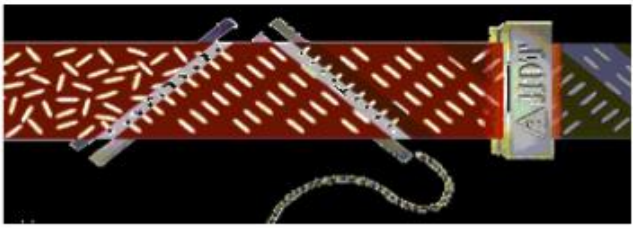
| | Descripción | No. de caracteres | Valor |
|---|---|---|---|
| CI | Centinela inicial | 1 | oBh |
| CF | Código de formato | 2 | |
| PAN | Número de cuenta principal | 19 | |
| CS | Campo separador | 1 | oDh |
| Nombre | Nombre | 26 max. | 3Eh |
| Add Data | Código de país (opcional) | 3 | |
| | Código de moneda | 3 | |
| | Exponente de moneda | 1 | |
| | Monto autorizado por ciclo | 4 | |
| | Monto remanente del ciclo | 4 | |
| | Inicio del ciclo (fecha valida) | 4 | |
| | Longitud del ciclo | 2 | |
| | Cuenta de intentos | 1 | |
| | PIN control de parámetros | 6 | |
| | Controles de intercambio | 1 | |
| | Restricciones de servicio PAN | 2 | |
| | Restricciones de servicio SAN-1 | 2 | |
| | Restricciones de servicio SAN-2 | 2 | |
| | Fecha de expiración (opcional) | 4 | |
| | Número de secuencia de tarjeta | 1 | |
| | Número de seguridad de la tarjeta | 9 | |
| Diss Data | No. Primera cuenta subsidiaria (opcional) | | |
| | No. Segunda cuenta subsidiaria (opcional) | | |
| | Marcador de relevo | 1 | |
| | Digito de control criptográfico | 6 | |
| | Datos discreto | | |
| CF | Centinela final | 1 | oFh |
| LRC | Carácter de verificación de redundancia longitudinal | | |

### Seguridad de banda magnética

La seguridad utilizada en las bandas magnéticas es por lo general tecnología propietaria y costosa, dentro de las técnicas más comúnmente utilizadas están: Marca de agua magnética (Watermark Magnetics ®), XSec, Holomagnéticos, XiShield, Jitter Enhancement, ValuGard, MagnePrint® entre otras (ver figura 3.13).




Tarjeta con MagnePrint®



Tarjeta con marca de agua - Watermark Magnetics ®

Figura 3.13 Seguridad en banda magnética

Estos mecanismos de seguridad sobre la banda magnética ayudan a enmascarar los datos contenidos dentro de las pistas de las tarjetas, y hace que sean ilegibles de forma directa.

### Tarjetas con microchip

El microchip o circuito integrado es una pastilla pequeña de material semiconductor, de algunos milímetros cuadrados de área, sobre la que se fabrican circuitos electrónicos.

Las tarjetas con chip y código son tarjetas que integran un pequeño microchip al frente de la tarjeta. Este tipo de tarjeta es más segura que las tarjetas que se fabrican con banda magnética. Las tarjetas con chip y código requieren un número de código asociado con la tarjeta para verificar la transacción bancaria, ya que se procesa de manera diferente que las realizadas con la tarjeta magnética. Las tarjetas con chip y código se insertan en la terminal en lugar de ser pasadas.

El comprador ingresa el código en lugar de firmar un recibo para verificar el cambio.

Las firmas internacionales MasterCard, Visa, y Europay publicaron un estándar de interoperabilidad para el pago con tarjetas inteligentes en 1996, que fue revisado en 2000. Este estándar, llamado EMV se ha introducido de manera gradual en todo el mundo, con la esperanza de reemplazar las tarjetas basadas en bandas magnéticas. Actualmente, las especificaciones EMV son costosas de implementar, con el único beneficio de la reducción del fraude.

Es necesario distinguir entre tarjetas inteligentes y tarjetas con chip, ya que el chip no es lo que hace "Inteligente" a una tarjeta, si no el microprocesador, por ello existen diferentes tipos de tarjetas según el tipo de circuito integrado con el que cuenten, unas son "Inteligentes" y otras son de "memoria".

Así se tienen:

- Tarjetas con circuito integrado de Memoria. (Tarjeta con Chip).
- Tarjetas con circuito integrado con Microprocesador. (Tarjeta Inteligente).

Las tarjetas inteligentes son tarjetas plásticas que contienen un pequeño microprocesador, capaz de hacer diferentes cálculos: guardar información, manejar programas y está protegido a través de mecanismos avanzados de seguridad. Estas tarjetas con circuito integrado, pueden contar con aplicaciones financieras, para ser utilizadas como medio de pago.

## Números de la tarjeta

Es el número de cuenta principal de las tarjetas bancarias (crédito o débito básicamente). Tiene una cierta estructura interna y un sistema común de numeración. Los números de tarjeta de crédito son un caso especial de la norma ISO/IEC 7812 números de tarjetas bancarias.

La norma ISO/IEC 7812 establece la conformación de los números de tarjeta, compuesto básicamente por un número o dígito como identificador principal de la Industria (MII), de uno a seis dígitos el Número de Identificación del Emisor (IIN), un número de cuenta y un digito verificador de un solo número calculado utilizando el algoritmo de Luhn. El MII es considerado como parte del IIN.

El término "Emisor Número de Identificación" (IIN) sustituye a los utilizados anteriormente "Número de Identificación Bancaria" (BIN). La norma ISO / IEC 7812 contiene más información al respecto para más información.

El número de tarjeta es conocido comúnmente llamada en la industria como el número de cuenta principal (PAN por sus siglas en ingles). En la siguiente tabla 3.14 se observa cómo se conforma este número.

Tabla 3.6 Composición del PAN

| Identificador Mayor de Industria (MII) | Número Identificador de Emisor (IIN) | No. Cuenta | Digito verificador |
|---|---|---|---|
| 1 digito | 5 digitos | Max. 12 digitos | 1 digito |

En términos generales una tarjeta consta de 16 dígitos, como por ejemplo, la imagen que se muestra en la figura 3.14 Los 16 números están separados en grupos de 4, la razón de formar grupos de 4 es solo para poder identificar mejor los bloques, es decir, no es porque cada grupo tenga un significado.


Figura 3.14 Tarjeta bancaria

El significado de esos 16 números es el siguiente:

- Los cuatro primeros dígitos (1234) son el número de identificación de la entidad que proporciona la tarjeta, que es diferente según la entidad a la que corresponde (hasta siendo de la misma entidad, dos tarjetas de distintos continentes pueden tener números distintos).

- El siguiente dígito, (5) indica el tipo de tarjeta y la entidad financiera a la que corresponde (American Express, VISA, entre otros).

- Los diez dígitos posteriores (6781234567) corresponde al número de identificación del usuario o en algunos casos el número de cuenta al que pertenece la tarjeta, que lo identifican de forma única.
- El dígito final (8) es un dígito de control verificador único por cada tarjeta y número de PAN.

## 3.5.9 Proceso adquirente-emisor

De acuerdo a las estádisticas publicadas por BANXICO en el 2014, los pagos con tarjetas bancarias de crédito y de débito en comercios y prestadores de servicios han venido ganando importancia en los últimos años en México, durante 2006 se realizaron más de 530 millones de pagos con tarjetas bancarias en comercios con un valor de 299 mil millones de pesos. El valor de dichas transacciones en 2006, representó el 3.9% del PIB y el 5.6% del monto del consumo privado. Esto ha fomentado el crecimiento de los medios de pagos.

Así, durante 2013 se realizaron más de 1,676 millones de pagos con tarjetas bancarias en comercios con un valor de 811 mil millones de pesos constantes de 2013. El valor de dichas transacciones en 2013, representó el 5.8% del PIB y el 8.5% del monto del consumo privado.

A continuación se describen de manera general los procesos que se llevan a cabo entre las entidades emisoras y clientes, estos procesos son conocidos como compensación y liquidación y se ejecutan detrás de una operación bancaria (pago en comercios, retiros en cajeros, transferencia interbancaria entre otras operaciones) con ellos se realiza el pago a las marcas, emisores, adquirentes y entre los bancos. Para lo anterior se definen algunos conceptos claves que se utilizan para explicar el proceso de compensación y liquidación.

### Conceptos preliminares

**Emisor:** el emisor es la institución financiera que inicia y mantiene relaciones con los consumidores, es quien está autorizado para emitir las tarjetas bancarias, y autorizar los consumos u operaciones bancarias efectuadas con la tarjeta.

**Adquirente:** institución financiera que afilia, provee servicios y mantiene acuerdos contractuales con los comercios afiliados para aceptar y procesar transacciones con las tarjetas bancarias.

**Tarjeta habiente:** es quien posee una tarjeta bancaria otorgada por una institución financiera en este caso el banco emisor, para realizar el pago de bienes y servicios en comercios afiliados.

**Visa:** institución financiera, que ofrece productos y servicios a las entidades miembros y no se relaciona directamente con los consumidores. Visa brinda a las instituciones financieras miembros los elementos necesarios para operar de manera global.

**Incoming:** es un archivo batch generado de todas las transacciones realizadas con las tarjetas de nuestros clientes en otros países. Este archivo permite el desglose las operaciones financieras y de las transacciones realizadas.

**Outgoing:** es el archivo generado por el emisor, donde se encuentra todas las transacciones realizadas por los tarjeta habientes de otros bancos en ATM's propios de la institución. También se envían los contra cargos y aclaraciones.

### Sistema de pago

Se le nombra sistema de pagos, al conjunto de instrumentos y procesos bancarios que se usan para transferir dinero, el buen funcionamiento y la seguridad que brinden hacen que la gente tenga confianza y les facilita las actividades económicas (pagos, transferencias, depósitos, etc.).

Los sistemas de pagos interbancarios se basan en un contrato que los participantes firman con el operador del sistema. Además del operador del sistema y de los participantes, interviene un agente liquidador que lleva las cuentas de los participantes donde carga y abona el importe correspondiente a los pagos para liquidarlos. En México el agente liquidador para varios sistemas es el Banco de México.

En México, los sistemas de pagos procesan millones de transacciones todos los días, y algunas de ellas, se hacen por cientos de millones de pesos. Claramente, la actividad económica sería muy distinta sin los sistemas de pagos.

## Medios de pago

Un medio de pago, es generalmente un activo que se puede usar como dinero. Desde luego los billetes y monedas son medios de pago. Otro medio de pago puede ser un depósito bancario.

## Pagos con tarjetas

Las tarjetas de crédito son instrumentos de pago asociados a una línea de crédito que un banco otorga a su cliente, el cual la ejerce al pagar bienes y servicios o disponer de efectivo, con su tarjeta. Las tarjetas de débito son instrumentos similares, pero en vez de estar asociadas a una línea de crédito, los están a una cuenta corriente. Las terminales electrónicas que tienen instalados los establecimientos para recibir pagos aceptan prácticamente cualquier tarjeta de crédito o débito. Estas terminales se denominan Terminales Punto de Venta, TPV. Los tarjetahabientes también pueden obtener dinero con sus tarjetas en cualquier cajero automático de los bancos, independientemente de cuál sea el banco que emitió la tarjeta, aunque si el banco dueño del cajero es distinto al emisor de la tarjeta la comisión que pagará el cliente por el uso del cajero será mayor. En los pagos con tarjetas participan varias entidades con roles distintos: a) el Banco Emisor es el banco que emite la tarjeta asociada a un contrato de crédito o a una cuenta corriente. Este banco pagará el importe de la compra al comercio donde se utilizó la tarjeta; b) el Banco Adquirente es el banco que lleva al comercio una cuenta en la que depositará los importes de las compras con tarjetas, y se encarga de administrar la terminal electrónica instalada en el comercio para procesar las compras en línea; c) los Procesadores son empresas que proporcionan los servicios de comunicación entre los Bancos Emisores y los Adquirentes; y d) las Marcas, quienes establecen los estándares operativos y financieros que los Bancos Emisores deben cumplir para poder llevar la marca en la tarjeta.

Cualquier banco mexicano puede emitir tarjetas y proporcionar servicios a los comercios para que acepten pagos. Prosa y E-global son los procesadores que operan en el país, cada uno de ellos da servicios de comunicación y proceso de operaciones de pago con tarjetas a varios bancos Emisores y Adquirentes. Una tarjeta bancaria emitida en México puede llevar una de las siguientes marcas: MasterCard, Visa o Carnet.

## Funcionamiento de las redes de pagos con tarjetas

En los siguientes diagramas se presenta la operación y funcionamiento de la red de pagos. La figura 3.15 se ilustra el flujo de una transacción interbancaria.


Figura 3.15 Transacción bancaria efectuada con tarjeta bancaria

En la tabla 3.7 se describe el proceso de autorización para unas transacciones interbancarias.

Tabla 3.7 Proceso de una transacción financiera

| # | Descripción |
|---|---|
| 1 | El consumidor en este caso el tarjetahabiente utiliza su tarjeta como medio de pago para realizar una operación financiera |
| 2a | A través de la TPV o cajero automático (ATM) se solicita al banco, en este caso banco adquirente la autorización para realizar la operación financiera (pago, abono, compra, retiro). |
| 2b, 2c | El Adquiriente envía la autorización al banco que proporcionó la tarjeta al consumidor, conocido como Banco Emisor; la solicitud de autorización se envía a través de un procesador de pagos con tarjetas. |
| 3, 4a | El Emisor verifica el saldo de la cuenta de la tarjeta, aplica el cargo por el monto de la operación financiera autorizada y envía la autorización al procesador. |
| 4b, 4c | El procesador transmite la autorización al Adquiriente, y éste al Comercio (TPV) y en el caso de cajero automático se refleja la transacción de manera casi inmediata. |
| 6 | La TPV o cajero automático imprime su comprobante de transacción u operación financiera efectuada. |

En el siguiente diagrama de la figura 3.16 se ejemplifica el flujo del proceso de compensación y liquidación. El proceso de compensación y liquidación es el proceso que se efectúa entre los bancos emisores, bancos adquirentes y procesadores de medios de pagos con la finalidad de garantizar que las operaciones bancarias realizadas por los tarjetahabientes estén aprobadas y realizadas por cada respectivo banco del tarjetahabiente. En términos generales compensa y liquida a cada banco las operaciones financieras realizadas por los tarjetahabientes.

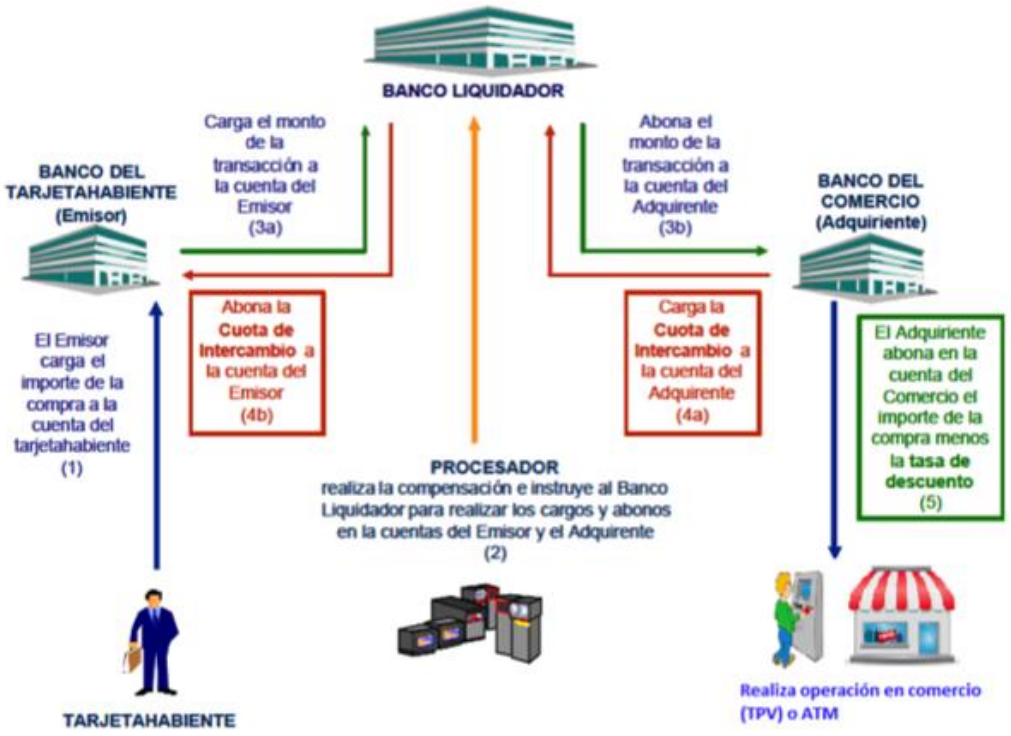



Figura 3.16 Compensación y liquidación

En la tabla 3.8 se describe el proceso de compensación y liquidación.

Tabla 3.8 Proceso compensación y liquidación

| # | Descripción |
|---|---|
| 1 | El Banco Emisor carga el monto de la compra a la cuenta (de crédito o débito) del tarjetahabiente. |
| 2 | El Procesador de Tarjetas realiza la compensación e instruye al Banco Liquidador a realizar las siguientes operaciones:<br>✓ Cargar el monto de la transacción a la cuenta del Banco Emisor (3a).<br>✓ Abonar el monto de la transacción a la cuenta del Banco Adquiriente (3b).<br>✓ Cargar a la cuenta del Banco Adquiriente el monto de la Cuota de Intercambio asociada a la transacción. Esta cuota la paga el Adquiriente al Emisor como compensación por el uso de la tarjeta (4 a)<br>✓ Abonar a la Cuenta del Banco Emisor el monto de la Cuota de Intercambio asociada a la transacción (4b). |
| 5 | El Banco Adquiriente deposita en la cuenta del Comercio el monto de la transacción menos una comisión por sus servicios denominada tasa de descuento. |

Es necesario tener presente que la figura de banco liquidador en México, es Banco de México (BANXICO). Al finalizar el proceso de “Compensación y Liquidación de una transacción interbancaria” el efecto neto para cada una de las partes involucradas es el siguiente: el Tarjetahabiente paga el Importe de la Compra; el Comercio recibe el Importe de la Compra menos la Tasa de Descuento; el Banco Emisor obtiene la Cuota Interbancaria y el Banco Adquiriente recibe la Tasa de Descuento menos la Cuota Interbancaria. Cabe destacar que los Bancos Emisor y Adquiriente pagan una comisión al “Procesador de pagos con tarjetas" (En México existen dos procesadores de pagos con tarjeta E-Global y PROSA, dichos procesadores se conocen con el nombre de camaras de compensación) por sus servicios. En el caso de una transacción mismo banco, el flujo es el siguiente como se muestra en la figura 3.17.


Figura 3.17 Operación bancaria mismo banco

En la tabla 3.9 se describe el proceso de una operación bancaria realizado con una tarjeta bancaria cuyo banco emisor del tarjetahabiente es el mismo del comercio o del ATM.

Tabla 3.9 Proceso operación bancaria mismo banco

| # | Descripción |
|---|---|
| 1 | El tarjetahabiente utiliza su tarjeta bancaria en un comercio o cajero automático. |
| 2 | El comercio , a través de su terminal punto de venta (TPV), solicita al Adquiriente autorización para cargar tarjeta. En el caso de la operación realizada en cajero automático valida con el adquirente los datos del tarjetahabiente. |
| 3 | Dado que el Adquiriente es el Emisor, éste verifica el saldo y carga la cuenta de la tarjeta por el importe total de la compra u operación bancaria solicitada (pago, deposito, retiro, transferencia). |
| 4 | Asimismo autoriza la operación bancaria solicitada. |
| 5 | Se imprime el comprobante e la operación bancaria efectuada. |
| 6 | En algunos casos el pagaré o comprobante es firmado por el tarjetahabiente |
| 7 | En el caso de las operaciones efectuadas en comercios, el adquirente abona en la cuenta del comercio el importe de la compra. En los cajeros automáticos el adquirente realiza la operación bancaria solicitada. |

En este caso no interviene el procesador ni banco liquidador. Este caso se presenta cuando los procesos adquirentes y emisor los efectúa el mismo banco. En el caso de cajeros automáticos se presenta cuando la red de cajeros pertenece al mismo banco. En México, aproximadamente el 67% de las transacciones son interbancarias y el 33% son mismo banco, según información publicada por BANXICO en el 2014.

## 3.6 Desarrollo del proyecto

Como se comentó anteriormente en el presente capítulo se describe paso a paso el trabajo desarrollado durante este proyecto, haciendo énfasis en la arquitectura y esquema de cifrado diseñados. El proyecto en su totalidad esta conceptualizado en tres fases diferentes.

El caso de estudio presentado en este trabajo explica las dos primeras fases. Estas se exponen y detallan a continuación. La tercera fase consiste en la expansión del servicio teniendo como meta en el 2015 instalar alrededor de 50 cajeros (las fechas y calendario se encuentra en definición), la cual a la conclusión de este trabajo está en negociación los términos, condiciones, las responsabilidades y financiamiento.

## FASE I

Consiste en diseñar y conceptualizar toda la arquitectura necesaria que se requiere implementar para brindar el servicio. Como representante del área de seguridad de la información y responsable de diseño y esquema de seguridad es necesario visualizar los controles necesarios que se deben efectuar para cumplir con un proceso que garantice la confidencialidad, integridad y disponibilidad del servicio.

En esta primera fase se definió lo siguiente:

- Equipo de trabajo
- Arquitectura de red
- Arquitectura de seguridad
- Arquitectura de apliaciones

Mi participación consistió en definir la arquitectura de seguridad. Considerando el esquema y tecnología de cifrado.

### Preparación

Como primer punto importante, se analizó la arquitectura y elementos con los que se contaba, en este sentido en la siguiente figura 3.18 se muestra la infraestructura de cifrado que se tenía implementado en la plataforma transaccional y se observa el propósito específico de los equipos de cifrado.

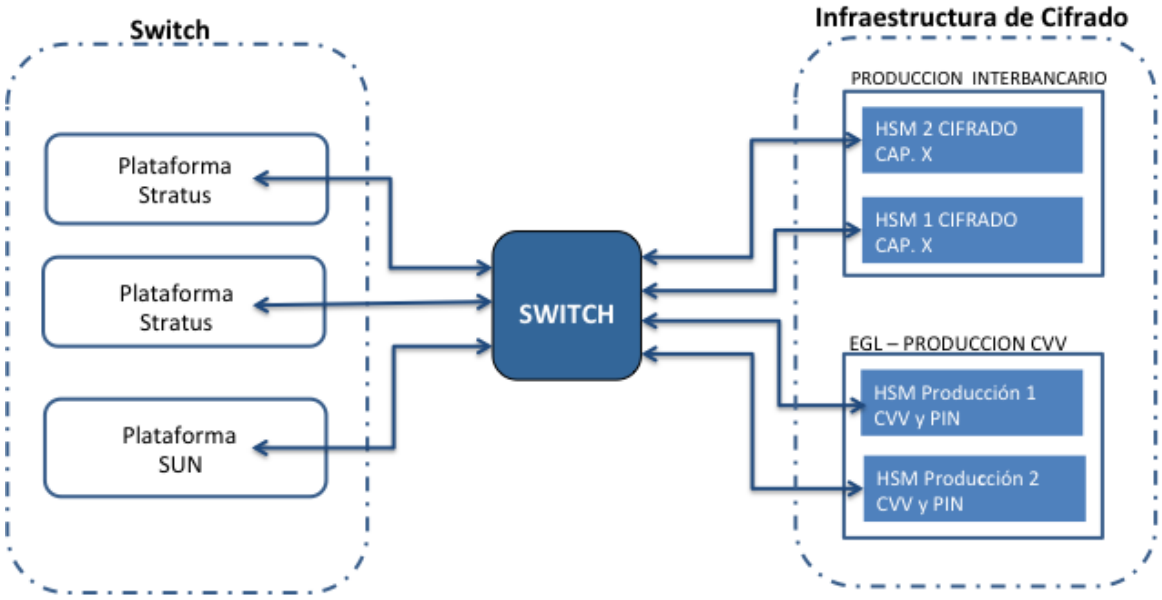



Figura 3.18 Conexión de HSM

Se contaba con dos equipos HSM que son utilizados para cifrar las transacciones de comercios realizadas a través de TPV´s o PIN pad (HSM 1 y 2 de CIFRADO) conectados a los sistemas autorizadores (stratus y SUN) en alta disponibilidad, estos sistemas autorizadores son los encargados de procesar las transacciones. Adicional se observan otros dos equipos HSM utilizados para cifrar las operaciones financieras donde se valida el CVV (Card Verification Value) y PIN (Personal Identification Number) (HSM 1 y 2 de Producción CVV y PIN), estos equipos de igual manera están conectados al sistema autorizador en alta disponibilidad. Los equipos HSM utilizados son THALES certificados FIPS 140-2. (Ver figura 3.19)

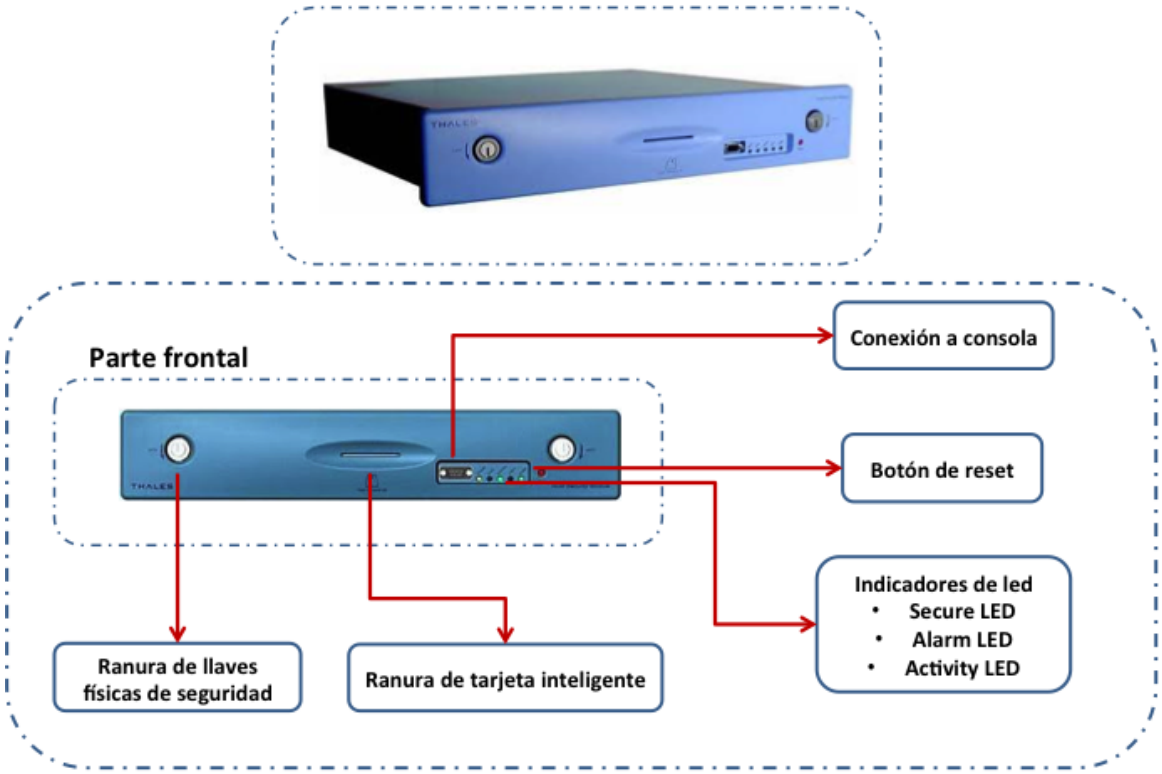



Figura 3.19 Modelo Thales

El proceso de ejecutar/autorizar transacciones de forma casi inmediata se le conoce como proceso de línea. La capacidad de procesamiento de los equipos HSM se mide en transacciones (TX) X segundo, los equipos descritos anteriormente tienen una capacidad de 850 TX X segundo.

En el diagrama de la figura 3.19 se visualiza la infraestructura de cifrado este esquema no soporta las transacciones de ATMs. Esto fue una primer limitante en el diseño del proyecto. Como respuesta a esta dificultad, se optó por utilizar equipos HSM de la marca REALSEC, estos equipos de igual manera cuentan con la certificación FIPS 140-2 (ver figura 3.20) y la capacidad de estos equipos es de 600 TX por segundo y se cuentan con dos equipos lo que hace que la capacidad se eleve a 1200 TX por segundo.

Con la finalidad de validar el funcionamiento y operación de los equipos REALSEC, estos se instalaron en un laboratorio para tener un ambiente de desarrollo controlado.

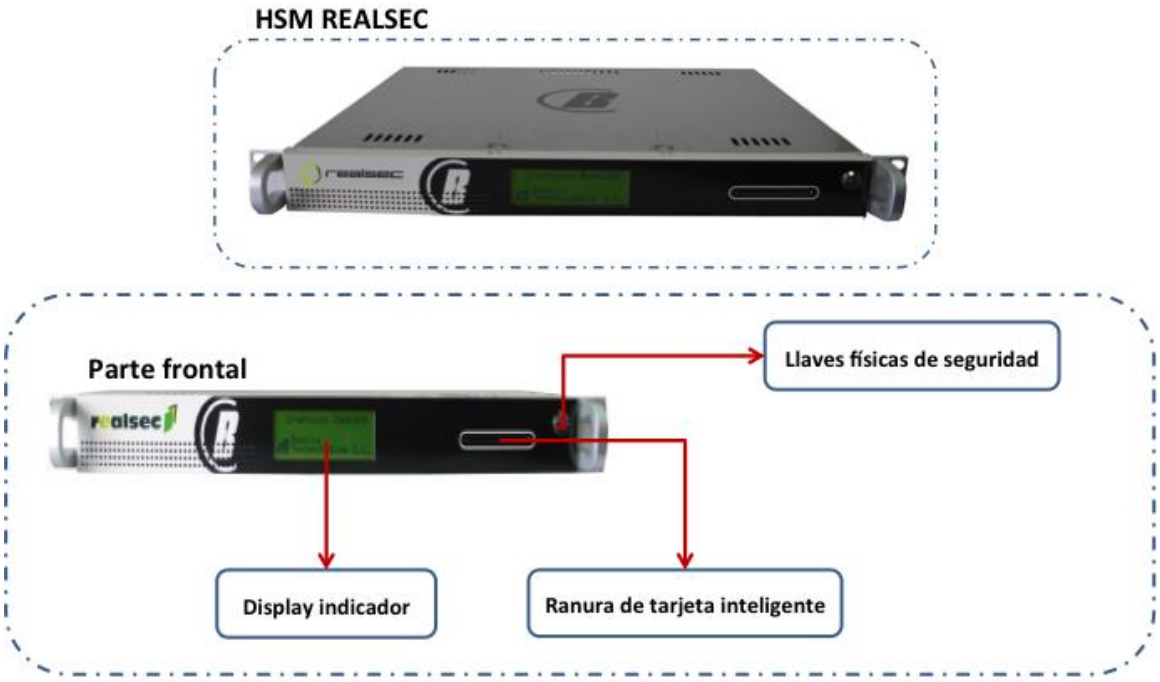



Figura 3.20 Modelo Realsec

## Desarrollo del proyecto

Como parte de una estrategia de negocio para incursionar en nuevos nichos de mercado, en enero del 2013 Eglobal empieza a diseñar el esquema necesario con la finalidad de iniciar una nueva era, esto es ofrecer el servicio de ATM´s a nivel de switch para el primer trimestre del 2015, actualmente en México la única empresa que brinda el servicio es PROSA, las reglas del mercado financiero han cambiado, dentro de las que destaca las siguientes:

- Apertura para incorporar mas camaras de compensación en México
- Cobros estandirazados y regulados por BANXICO
- Apertura para brindar servicios independientes y adicionales a la camara de compensación.

Esto permite a Eglobal brindar nuevos servicios.

A continuación en la figura 3.21 y 3.24 se ilustran las actividades que se realizaron en esta primera fase. Las primeras actividades de la fase1 dieron inicio a principios del año 2013 y terminaron en agosto del 2013. Las actividades de la fase 1 se realizaron de acuerdo a lo planeado. En la figura 3.22 se muestra un extracto de la bitácora del seguimiento del proyecto.

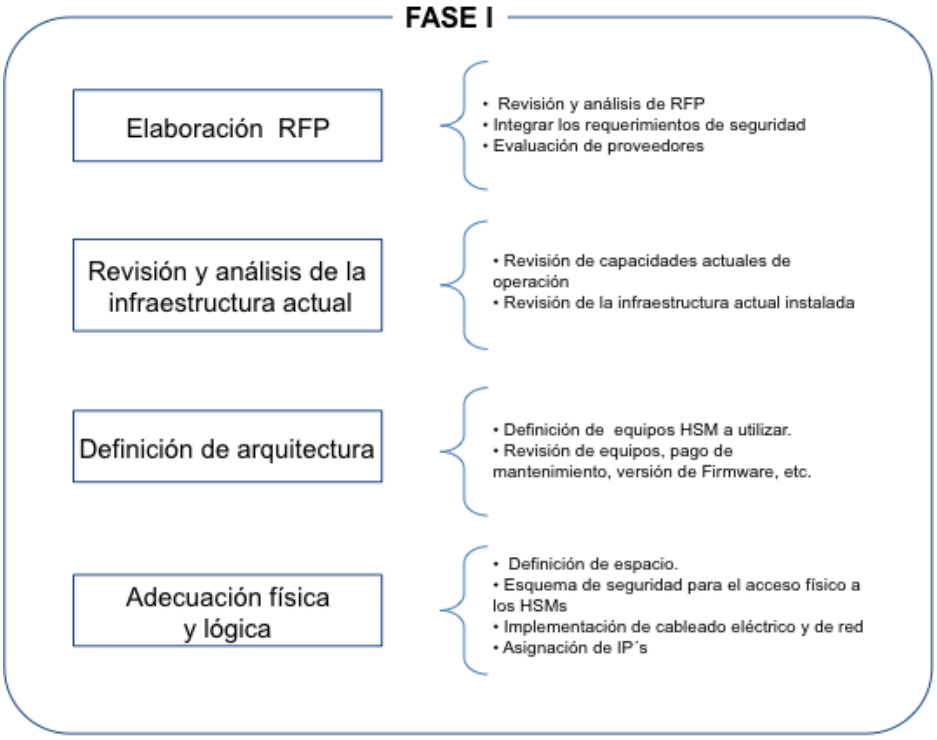



Fig. 3.21 Fase I – Desarrollo fase 1 (parte 1)

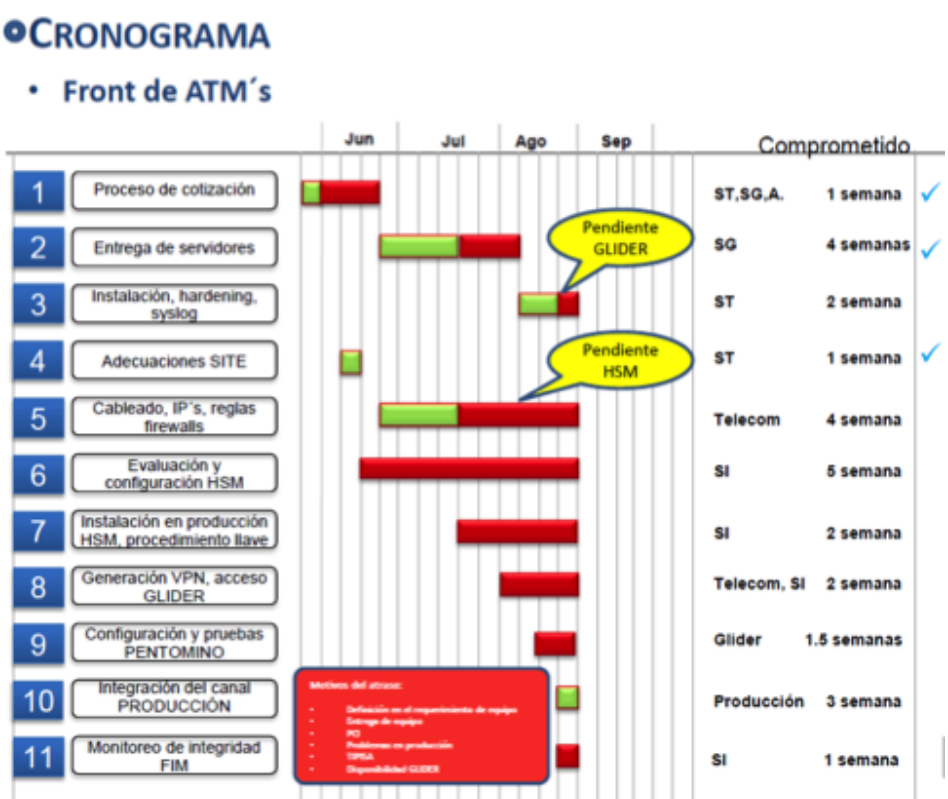



Figura 3.22 Cronograma del proyecto

En esta primera parte lo que destaca son los requerimientos de seguridad solicitados en el RFP así como las características y adecuaciones físicas solicitadas, las cuales fueron necesarias cubrir en la instalación de los HSM´s. Esta primera fase se desarrolló a partir de Marzo del 2013 y concluyó en agosto del 2013 con una duración de cinco meses logrando terminar en el tiempo estimado las actividades planeadas.

Algunas de las características de adecuaciones físicas importantes y necesarias que se cubrieron fueron las siguientes:

- Implementar control de acceso físico biométrico con base en huellas digitales, y solicitud por escrito previa para otorgar acceso a laboratorio.
- Separación física entre otros dispositivos del laboratorio. Es decir que los dispositivos de TI utilizados se encuentre en un rack diferente y único.
- Cámaras de vigilancia con grabación de video constante (24*7*365) y almacenamiento de un año.

Se incluyó una evaluación de seguridad al proveedor, por medio de este se solicita que responda las preguntas para evaluar los controles de seguridad y validar el grado de cumplimiento de la solución, en la figura 3.23 se muestra un extracto del cuestionario de evaluación.

| A |
|---|
| E-GLOBAL RFP - POS & ATM TRANSACTIONAL PLATFORM |
| 9. INFORMATION SECURITY. |
| 9.1. GENERAL. |
| **9.1.1.** List the native security tools included in the solution and a brief description |
| **9.1.2.** List the external security tools that is recommended to be adquired in order to improve security and/or meet Security Compliance |
| **9.1.3.** Is there documentation, checklists or procedures in order to establish a security baseline (security hardening) |
| 9.2. SEPARATION OF DUTIES. |
| **9.2.1.** Is the solution capable of implementing separation of duties based on business needs (Ex. Administrative,Operative, Monitoring/Security Users, Established Roles, Permmisions Assigment, etc.) |
| **9.3.2.** How Is the application control access system implemented? Is independent or depent to the OS? . |
| 9.3. PROTECT SENSITIVE DATA. |
| **9.3.1.** What are and how can you control the parameters of debug/flow control/storage sensible information in the solution? (Transaction logs - History files - Trace files - Debugging logs- Database contents) |
| **9.3.2.** Is there any native utility for secure deleting information related to sensitive data in order to make it unrecoverable. |
| 9.4. INTEGRITY. |
| **9.4.1.** How can you protect the integrity of the files involved in the solution (Ex. Programs,logs,etc). |
| **9.4.2.** The application is able to show proof of tracking in every configuration change? (It is performed native or need to purchase anotther module/functionality) |
| 9.5. REMOTE ACCESS. |
| **9.5.1.** How the remote access support is provided? (shell, graphical interface,etc) |
| **9.5.2.** What are the access controls related to remote access support? |

Fig. 3.23 Evaluación de seguridad

Continuando con la descripción de actividades en la figura 3.24 se presentan las siguientes acciones realizadas.

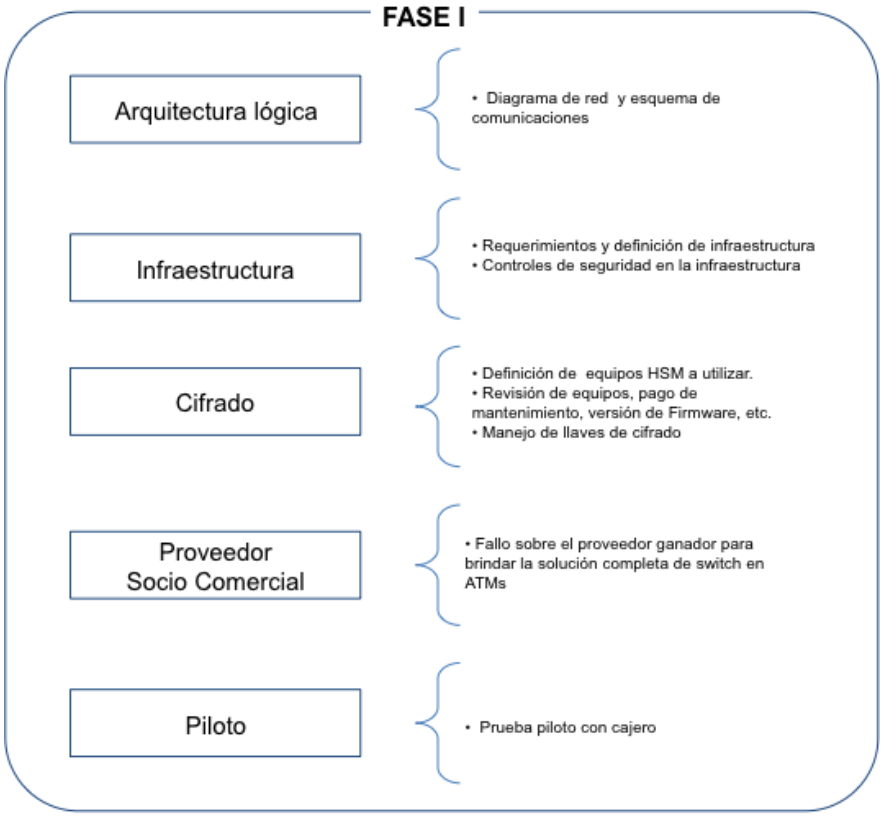



Fig. 3.24 Fase I – Desarrollo fase 1 (parte 2)

Estas actividades iniciaron de acuerdo a lo planeado en octubre del 2013 y finalizaron en febrero del 2014. Lo importante a destacar fue la definición del fallo para la elección del proveedor ganador, quien será responsable de brindar la solución comercial y participará como socio comercial para la interconexión de cajeros automáticos. Esta fusión permite a Eglobal ampliar el mercado y brindar la solución en un tiempo menor y a un bajo costo.

La fusión permite a Eglobal generar una estrategia comercial, en la cual el socio costea mano de obra (desarrolladores), arquitectura y dispositivos de TI necesarios, y Eglobal costea espacio e implementación además de contar con una cartera de clientes potenciales para ofrecer el servicio. Esto permite a Eglobal no generar un gasto fuerte de inversión para comparar equipo o infraestructura de TI y la contratación de personal para el desarrollo del proyecto.

Con respecto a la arquitectura de servidores, el área de infraestructura de TI definió la arquitectura de acuerdo al RP y especificaciones del socio comercial, por parte de seguridad se definió la infraestructura de cifrado a utilizar, los mecanismos y controles de seguridad necesarios aplicar sobre la infraestructura de TI.

Debido a que en este ambiente se manejarán datos de tarjetahabiente se define como ambiente PCI y por tanto los controles de seguridad que se aplican son más estrictos.

Los principales mecanismos de seguridad que se aplican son:

- Escaneo de vulnerabilidades
- Configuración de syslog para el envío de logs al SIEM
- Monitoreo de integridad de archivos críticos
- Prueba de pentest o ethical hacking.

Un aspecto de seguridad muy importante fue definir la gestión de las llaves de cifrado (generación, carga y manejo de llaves y elementos criptográficos), si bien ya se tenía conceptualizado el hardware, es decir los HSM, fue importante definir los tipos de llaves y la gestión de las mismas, más adelante se describe el detalle de la arquitectura y elementos de cifrado utilizados.

Al final esta primera fase concluye con una prueba controlada en producción a manera de piloto en un cajero automático ubicado en un laboratorio de Eglobal.

## Arquitectura del proyecto

Para logar generar un ambiente de pruebas en un menor tiempo el socio comercial proveyó parte de la arquitectura de TI (servidores base de datos y aplicación). La infraestructura de Telecomunicaciones y cifrado fue provista por Eglobal.

En el siguiente diagrama de la figura 3.25 se visualiza de manera general el diagrama de conexiones. Las pruebas de conectividad y de flujo transaccional se realizaron con un banco cliente el cual presenta interés en el servicio de switch de cajeros que se desea implementar.

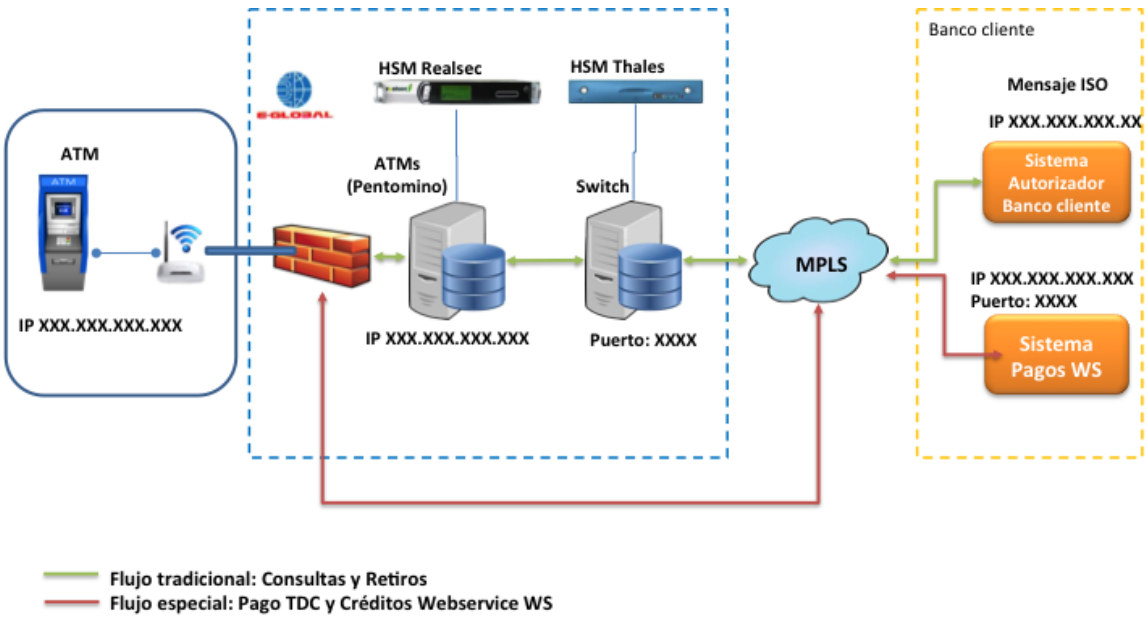



Fig. 3.25 Esquema de conectividad piloto

En el diagrama se identifican dos flujos para las transacciones (TX), el tradicional y el flujo especial, a continuación se describen ambos flujos:

- Flujo tradicional: el flujo transaccional, es decir las transacciones financieras se suelen manejar utilizando una mensajería estándar, la cual corresponde a la mensajería ISO8583.

- Flujo especial: éste fue diseñado para pagos de TDC y créditos del banco, el esquema fue diseñado de esta forma derivado que no se tienen los datos para autorizar dichas transacciones del banco. En este caso las transacciones son autorizados directamente por el banco cliente mediante un canal VPN.

Las transacciones financieras originadas con tarjeta son conformadas por el estándar internacional de mensajería ISO8583, es utilizado para intercambiar transacciones financieras electrónicas mediante procesadores (switch, en este caso Eglobal y Prosa).

Una transacción realizada con una tarjeta usualmente tiene como origen un dispositivo de compra, como una terminal POS, PINPAD o un cajero automático ATM, a través de una red (o redes) hacia el sistema emisor de la tarjeta para obtener una autorización en función de la cuenta del titular de la tarjeta. La transacción contiene información que se obtiene de la tarjeta (ejemplo, como el número de cuenta), la terminal (que puede ser el número de comercio), la transacción (por ejemplo, el importe) en conjunto con otra información que se puede generar o agregar dinámicamente por los sistemas que pudieran intervenir en el proceso. El sistema emisor de la tarjeta autoriza o rechaza la transacción, y genera un mensaje de respuesta que debe ser devuelto a la terminal en un tiempo breve (no mayor a 5 segundos).

ISO 8583 define un formato de mensaje y un flujo de comunicación para que diferentes sistemas puedan intercambiar estas transacciones. La mayoría de las operaciones realizadas en ATM usan ISO 8583 en algunos puntos de la cadena de comunicación, así como también las transacciones que realiza un cliente que usa una tarjeta para hacer un pago en un local. En particular, todas las transacciones se basan en el standard ISO 8583. La cadena ISO puede verse alterada durante algún punto cuando al mensaje se le necesite indexar un campo con la finalidad de indicar por ejemplo un balanceo de cargas, o la falta de disponibilidad del procesador central y se requiera realizar el desvío de la transacción. En una operación también puede verse alterada la cadena ISO, por ejemplo cuando se realiza una compra en algún súper mercado y adicional se realiza retiro de efectivo en caja, en este caso la cadena ISO se ve alterada y es llamada operación CASH BACK.

En términos muy generales un mensaje ISO 8583 consta de las siguientes partes:

- Message Type Indicator (MTI) - Indicador de Tipo de Mensaje
- Uno o más bitmaps, indicando qué elementos están presentes en el mensaje
- Data elements, los campos del mensaje

Si bien el mensaje ISO8583 se conforma por las partes antes mencionadas la forma de generar el mensaje ISO 8583 es un poco más compleja, en este trabajo no se mencionara la forma de generar este mensaje, basta con saber que este mensaje contiene información del tarjetahabiente y de la transacción financiera (TX) (compra, pago y venta principalmente), que es considera como sensible.

Al contener información de este tipo, la transmisión, el almacenamiento y procesamiento de este es manejado con medidas de seguridad muy altas. Durante la transmisión del mensaje se utilizan mecanismos de cifrado en las comunicaciones como enlaces VPN cifrados con IPSEC, enlaces dedicados como MPLS. Durante el almacenamiento también se utilizan mecanismos de cifrado.

Por norma general de la industria de medios pagos y la norma PCI los mensajes ISO8583 o cualquier otro que contenga datos de tarjetahabiente no pueden ser almacenados de forma indefinida o por largos periodos de tiempo, la TX solo se almacena durante el tiempo en que se procesa o ejecuta, posterior a este tiempo, debe ser eliminada utilizando mecanismos de borrado seguro.

Para el tiempo en el que la TX es transmitida y procesada se utilizan los módulos HSM, y para cifrar este tipo de mensajes entre las entidades financieras y procesadores de medios de pago se utiliza un algoritmo estándar acordado en la industria 3DES.

Cada módulo HSM maneja su nomenclatura muy específica para los tipos de llaves, sin embargo no importa el módulo HSM utilizado, cada uno de ellos maneja una tabla de equivalencia de llaves para cada hardware. En este caso se utilizaron dos tipos de hardware diferentes (THALES y REALSEC). En la siguiente figura 3.26 se visualiza un extracto de las tablas con los tipos de llave que manejan. Derivado de utilizar infraestructura distintas se tuvo que manejar esta tabla de equivalencias entre llaves para homologar los tipos de llaves necesarios a utilizar.

**Tabla de llaves - THALES**

| Variant ⇨ | | 0 | | | 1 | | | 2 | | | 3 | | | 4 | | | 5 | | | 6 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| LMK ⇩ | | G | E | I | G | E | I | G | E | I | G | E | I | G | E | I | G | E | I | G | E | I |
| Pair | Code | | | | | | | | | | | | | | | | | | | | | |
| 04 – 05 | 00 | ZMK | | | ZMK (Comp) | | | KML | | | | | | | | | | | | | | |
| | | A | | | U | A | U | U | A | U | | | | | | | | | | | | |
| 06 – 07 | 01 | ZPK | | | | | | | | | | | | | | | | | | | | |
| | | U | A | U | | | | | | | | | | | | | | | | | | |
| 14 – 15 | 02 | PVK TPK TMK | | | | | | | | | | | | CVK CSVK | | | | | | | | |
| | | U | A | U | | | | | | | | | | U | A | U | | | | | | |
| 16 – 17 | 03 | TAK | | | | | | | | | | | | | | | | | | | | |
| | | U | A | U | | | | | | | | | | | | | | | | | | |
| 18 – 19 | 04 | | | | DTAB | | | PB | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 20 – 21 | 05 | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 22 – 23 | 06 | WWK | | | | | | | | | | | | | | | | | | | | |
| | | U | A | U | | | | | | | | | | | | | | | | | | |
| 24 – 25 | 07 | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 26 – 27 | 08 | ZAK | | | | | | | | | | | | | | | | | | | | |
| | | U | A | U | | | | | | | | | | | | | | | | | | |
| 28 – 29 | 09 | BDK | | | MK-AC | | | MK-SMI | | | MK-SMC | | | MK-DAK | | | MK-DN | | | | | |
| | | U | A | U | U | A | U | U | A | U | U | A | U | U | A | U | U | A | U | | | |
| 30 – 31 | 0A | ZEK | | | | | | | | | | | | | | | | | | | | |

**Tabla de llaves -REALSEC**

| Tipo | Descripción | Operativa |
|---|---|---|
| LMK 0 | Clave Maestra | Cálculo KCV (6 caracteres) de la LMK 0 |
| LMK 1 | Claves de Custodio | Generación/Borrado |
| | | Importación/Exportación (RSA) |
| | | Importación/Exportación por componentes |
| | | Cálculo KCV (6 caracteres) |
| LMK 2 | Claves de Transporte de claves | Generación/Borrado |
| | | Importación/Exportación por componentes |
| | | Importación/Exportación cifrada con clave custodio |
| | | Importación/Exportación (RSA) |
| | | Cálculo KCV (6 caracteres) |
| LMK 3 * | Claves de Transporte de bloque de PIN | Generación/Borrado |
| | | Importación/Exportación cifrada con clave de transporte |
| | | Importación/Exportación (RSA) |
| | | Diversificación |
| | | Cálculo KCV (6 caracteres) |
| | | Conversiones del bloque de PIN |
| LMK 4* | Claves de PIN | Generación/Borrado |

Fig. 3.26 Tipos de llaves módulos HSM

En el siguiente diagrama de la figura 3.28 se ilustra el tipo de llaves que se utilizaron y resaltan las zonas de llaves y tipo de llaves utilizadas al transmitir el mensaje.

El concepto o término de zona de llaves es empleado cuando se refiere a la acción de transportar un mensaje cifrado bajo una llave que solo dos entidades pueden utilizar, esto es, se utiliza la clave que ha sido generada de forma compartida.

Lo anterior se refiere a que, son llaves que son generadas por dos entidades utilizando una llave por cada entidad, el resultado de esta es una llave única que solo puede ser generada utilizando el componente 1 de la entidad 1 y el componente 2 de la entidad 2. Obteniendo como resultado una llave única generada por componentes únicos.

Para transportar los mensajes de TX se tienen que generar llaves de zonas por componentes entre entidades, como se observa en el siguiente diagrama (figura 3.27).

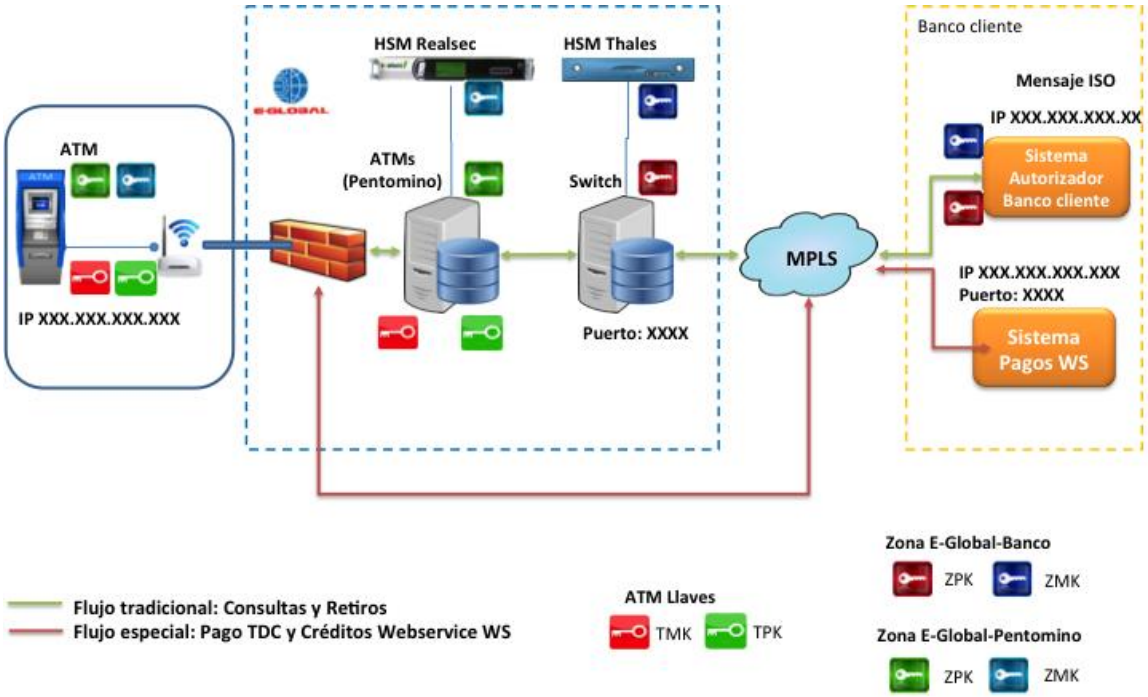



Fig. 3.27 Diagrama de llaves de cifrado

Las llaves utilizadas en el medio manejan una nomenclatura específica de acuerdo al producto utilizado, sin embargo manejan un estándar muy similar entre todos, de manera específica para este caso se manejan los siguientes tipos de llaves:

**ZMK** – Zone Master Key, llamada llave de zona o de transporte, utilizada generalmente para trasmitir mensajes cifrados por con una llave generada por esta misma ZMK.

**ZPK** – Zone Pin Key, al igual que la anterior es una llave de zona utilizada para trasportar el PIN de manera cifrada.

**TMK** – Terminal Encryption Key, llave que es utilizada para cifrar la TX en la terminal del cajero.

**TPK -** Terminal PIN Encryption Key, llave que es utilizada para cifrar el PIN.

**LMK** – Local Master Key, es la llave local maestra del equipo HSM, esta llave es única por cada equipo.

**Zona Eglobal-Pentomino**

Las llaves de esta zona se generaron de la siguiente manera:

- Para el HSM REALSEC:

  - Se genera ZMK por componentes en claro bajo la LMK del realsec.
  - Se genera ZPK cifrado bajo la ZMK generada en el punto anterior.

La llave ZMK generada anteriormente se requiere cargar en el aplicativo de Pentomino y se realiza la importación de llave la ZPK.

- Para el aplicativo de pentomino:

  - Se carga los componentes en claro de la llave ZMK generada en el HSM REALSEC. Se comprueba si la llave fue cargada con éxito validando el valor Check-Value (CVK) de la llave, con el valor CVK de la llave generada en el HSM REALSEC, si el valor CVK coincide de manera idéntica, quiere decir que las llaves fueron generadas y cargadas con éxito.

  - Se carga la ZPK bajo la LMK del HSM REALSEC.

Las llaves del ATM, se necesitan de la siguiente forma (estas llaves son generadas desde el HSM REALSEC):

- Para el ATM

  - Se genera componentes en claro para formar una llave TMK bajo la LMK del realsec. Los componentes son cargados en el cajero, si la carga de componentes fue correcta el valor CVK será idéntico al obtenido en el realsec.
  - Se genera una llave TPK cifrada bajo la TMK generada en el paso anterior. Esta llave se carga en el ATM.

Este par de llaves son utilizadas para inicializar el cajero, es decir con estas llaves se cifra un mensaje y empieza a establecer comunicación con el aplicativo Pentomino, si las llaves fueron generadas y cargadas de manera correcta el mensaje de prueba se procesará con éxito y se habrá logrado establecer de manera exitosa el canal de cifrado. Por cada TX se deriva una llave TPK' derivada, que será entendida por el aplicativo y procesará la TX, esta funcionalidad se realiza a nivel de desarrollo en aplicativo del Pentomino. Las llaves TPK y TMK fueron entregadas al banco cliente para que él mismo realizara la carga de llaves en el cajero ATM.

-Para el aplicativo Pentomino

- Se carga la llave de tipo TMK bajo la LMK del HSM REALSEC.
- Se carga La TPK bajo la LMK del HSM REALSEC.

Una vez que la TX es entendida por el aplicativo Pentomino, es enviada al Banco emisor cliente para su autorización, para este proceso se utilizan las llaves de zona ZMK y ZPK establecidas entre Eglobal y el banco emisor cliente. La TX se cifra bajo otras llaves de zona.

En el HSM REALSEC las llaves de tipo almacenamiento externo se cifran bajo la llave interna del HSM (LMK 2), para el caso de ZMK y TMK pertenecen al mismo grupo, es decir se cifran bajo la LMK 2. Las llaves ZPK y TPK también son del mismo grupo y se cifran bajo la LMK 3. Para el caso del HSM Thales corresponden al tipo de llave 000 para la ZMK, 001 para la ZPK, 002 para la TMK y TPK.

Una vez establecido todo el esquema de llaves y de realizar la carga de las mismas en los sistemas switch (plataforma transaccional), pentomino y ATM, se realizaron pruebas de transacciones financieras en ambiente de pruebas.

Debido a que todas estas actividades se generaron en un ambiente de pruebas no fue necesario generar acta de constancia de hechos.

## Resultados

En un periodo de 8 meses de enero a agosto del 2013 se logró implementar todo el esquema de desarrollo, la prueba realizada en un cajero ubicado dentro de las instalaciones de Eglobal fueron exitosas, esta prueba fue realizada en octubre del 2013, logrando realizar una operación de retiro en efectivo, pago de servicio y consulta de saldo. El retraso de la prueba obedeció problemas por parte del banco cliente para lograr los permisos para la instalación del cajero.

La conclusión de esta fase generó satisfacción a la empresa y se pudo mostrar la solución a clientes potenciales demostrando funcionalidad y disponibilidad del servicio en redes de cajeros automáticos que brinda Eglobal. El servicio de redes ATM se ha mostrado a diversos clientes y ha generado gran interés en ellos, como primer resultado se tiene ya negociada la implementación de este nuevo servicio en producción para un cliente banco. Por lo que el siguiente paso es implementar toda la arquitectura para un ambiente de producción certificada, como parte de la segunda fase.

## FASE II

La meta principal en esta fase es replicar la infraestructura construida en desarrollo en un ambiente de producción con los controles de seguridad que garanticen la confidencialidad, integridad y disponibilidad del servicio y el cumplimiento de las normas internacionales. Para lograr lo anterior se tuvieron que realizar cambios importantes, dentro de los que destacan los siguientes:

- Sustitución de los HSM realsec, por equipos de la marca Thales
- Instalación y configuración de la infraestructura nueva adquirida (pentomino).
- Prueba de pentest o ethical hacking sobre la infraestructura y aplicación.
- Definición de controles de seguridad.

A diferencia de la fase de desarrollo esta fase se contempla la separación de ambientes, es decir contar con equipos de propósito específico y controles de seguridad propios a cada ambiente de los sistemas, es decir controles de seguridad propios para la Base de Datos, para el aplicativo ATM y para el aplicativo WEB.

### Preparación

En la siguiente figura 3.28 las actividades a realizar en la fase II.

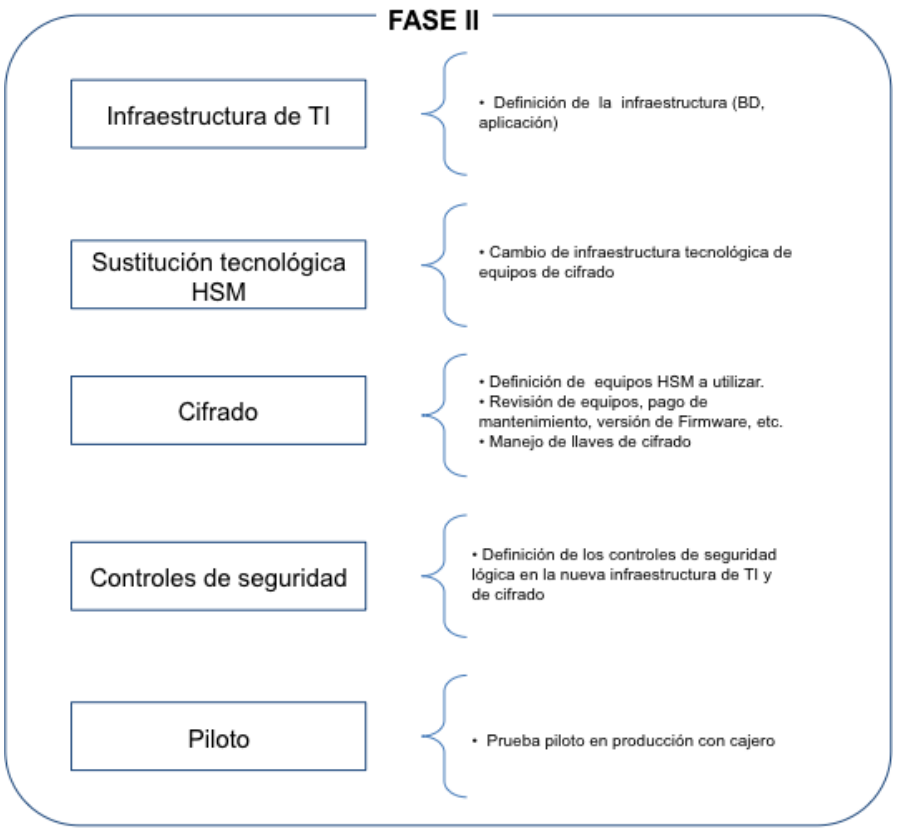



Fig. 3.28 Actividades Fase II

En esta segunda fase se contempla un cambio de infraestructura tecnológica, en la fase de pruebas y desarrollo se utilizaron equipos HSM realsec, las principales razones fueron, no tener equipos disponibles HSM Thales para realizar este tipo de pruebas y que no afectara al ambiente el desarrollo de otros servicios, además de no contar con un póliza de garantía, servicios profesionales, soporte y mantenimiento de estos equipos, y mantener una infraestructura homogénea de cifrado en producción, por estos motivos se impulsó el cambio de hardware de HSM.

Esto de alguna manera facilitó el intercambio de llaves de zona ya que no se utilizaría hardware diferente marcas.

Para contar con equipos disponibles, se tuvo que realizar una inversión de sustitución y renovación tecnológica para actualizar el hardware de cifrado actual en producción. El cambio consistió en remplazar los equipos actuales modelos HSM 8000 Thales por modelos HSM 9000 Thales, de esta manera se contaría con equipos disponibles. En el diagrama de la figura 3.19 se identifica la infraestructura en la cual se observa que se cuenta con 4 equipos de hardware de cifrado.

Como es una infraestructura que afecta al ambiente de producción y de misión crítica para la empresa, ya que como se mencionó, estos equipos cifran las transacciones, si ocurre un problema con estos equipos las transacciones serían rechazadas, lo que ocasionaría que alguna persona no pudiera efectuar su compra en alguna tienda departamental o comercio.

Bajo esta premisa se decidió sustituir dos equipos. Véase figura 3.29

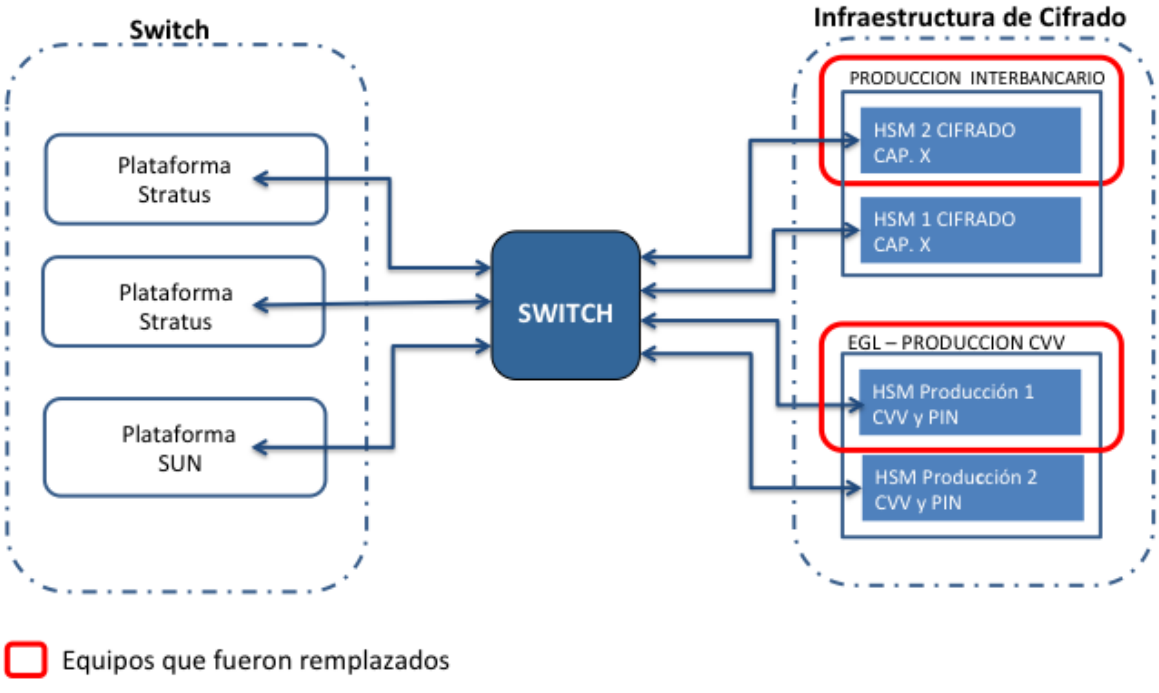



Figura 3.29 Remplazo de HSM

Con esta sustitución de equipos se logran obtener dos equipos HSM 8000 listos para instalarlos en producción y prepararlos para las TX en la red de cajeros ATM, adicional se renovó parte de la infraestructura con equipos de última generación.

Los equipos sustituidos (HSM 8000) cuentan con toda la funcionalidad para soportar el cifrado de TX en cajeros ATM, por lo que solo fue necesario realizar la renovación de póliza de garantía con el proveedor que incluye soporte en sitio y soporte de mantenimiento en caso de ser necesario.

En el siguiente diagrama (figura 3.30) es posible observar la infraestructura de cajeros instalada en el ambiente de producción.

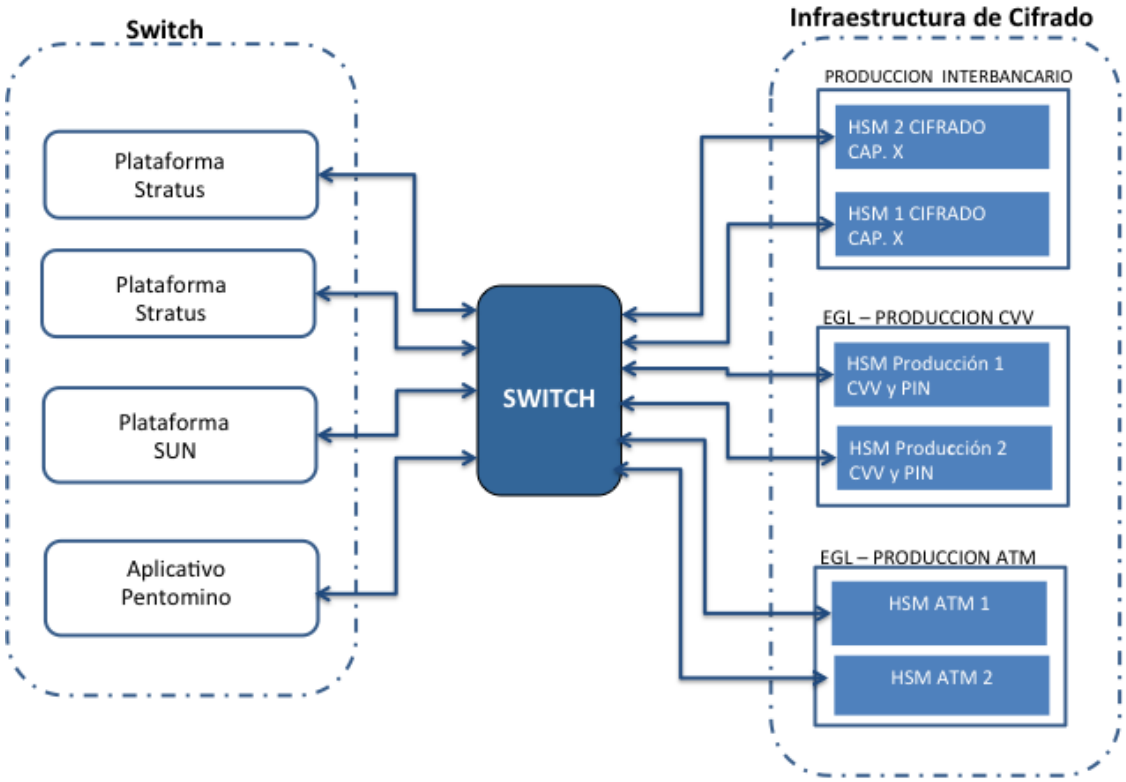



Figura 3.30 Remplazo de HSM

La propuesta es tener dos equipos HSM dedicados al cifrado de TX para cajeros ATM con la finalidad de tener un esquema de balanceo.

### Arquitectura de Pentomino

EL diagrama de red de comunicación de Pentomino con el switch transaccional y el HSM se representa en la figura 3.31.

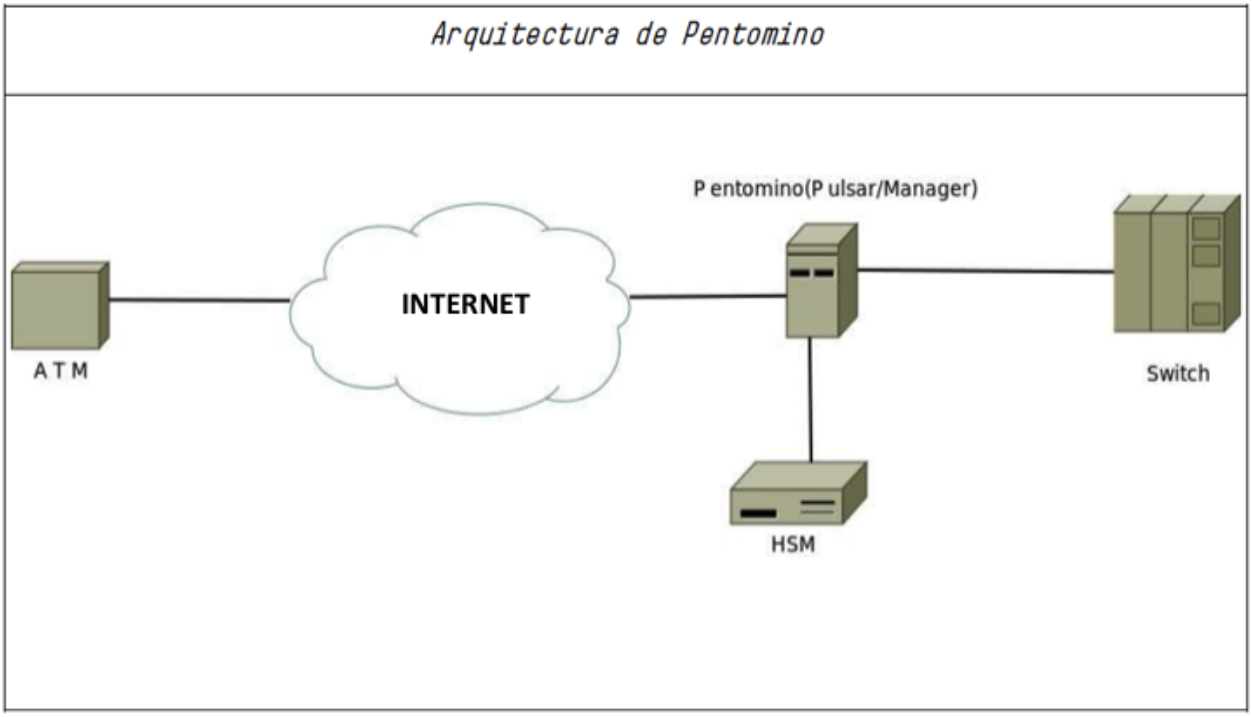



Figura 3.31 Diagrama de red Pentomino

El componente de Pulsar interactúa con el HSM para administración de llaves, a continuación se describen las funciones de los componentes que interactúan:

ATM. Automated Teller Machine. Cajero automático.

Pentomino. Software para la administración y operación de cajeros automáticos (ATM), Pentomino se compone a su vez, por dos subcomponentes:

- Pulsar. El componente de Pulsar tiene las funciones de ser un proxy hacia el Switch, transformar los mensajes de transacciones financieras del ATM a mensajes ISO8583 y Administrar las llaves de los ATM's y la llave de zona entre Pulsar y Switch.

- Manager. Este componente se encarga de la administración y configuración de ATM's, reportería, adquisición de logs de los ATM's, despliegue de los flujos y registros de los eventos de los dispositivos del ATM.

Switch. Procesador de transacciones financieras.

HSM. Hardware Security Module.

### Administración de llaves

La generación de llave maestra (transporte) y llave de trabajo (llave de cifrado para el PIN Block). Se lleva a cabo por medio de los siguientes pasos:

• Durante el proceso de instalación del cajero se introducen dos o más componentes de la llave maestra, previamente generada en el HSM (método de custodios).

• Con la llave maestra cargada en el PINpad del ATM, se inicia el intercambio de llaves de trabajo, enviando a Pulsar un mensaje para generar una llave de trabajo.

• Pulsar indica al HSM que genere una llave de trabajo cifrada con la llave maestra del ATM, una vez generada se la envía al ATM para que sea cargada en el PINpad.

• Cuando el PINPad tiene cargada la llave de trabajo, ya se puede empezar a transaccionar.

• En un periodo de tiempo establecido, se hará un cambio de llave de trabajo, Pulsar le pide al HSM que genere una llave de trabajo cifrada con la llave maestra del ATM.

• Pulsar notifica al ATM que cargue la nueva llave de trabajo.

Las llaves de trabajo y maestra son de doble longitud; 128 bits, el algoritmo que se utiliza de cifrado es 3DES.

### Importación de la llave maestra de zona (ZMK) y la llave de cifrado de PIN (ZPK).

La importación de la llave maestra de zona, se lleva a cabo por medio del proceso de custodios; dos o más custodios introducen los componentes de la llave de zona y después se valida el KCV. Pulsar importa al HSM los componentes para su validación y almacenamiento.

La importación de la llave de cifrado de PIN se realiza por el intercambio de llaves, una vez que se ha sincronizado la llave maestra en Pulsar y Switch. En el momento en que Pulsar recibe una notificación de nueva llave, este se la manda al HSM para su validación y almacenamiento.

La llave maestra de zona y de cifrado de PIN block, son de doble longitud: 128 bits, el algoritmo que se utiliza de cifrado es 3DES.

### Cambio de zona de PIN Block.

Cuando llega una petición de transacción financiera, Pulsar tiene que cifrar el PIN Block de la transacción con la llave maestra de zona, para realizar esto Pulsar pide al HSM que cambie el cifrado del PIN Block, indicando con que llave maestra del ATM viene cifrado y con cuál llave maestra de zona se desea cifrar.

**PIN Block**

El PIN Block se construye utilizando la función XOR mediante dos campos de 64 bits cada uno, y se utilizan diferentes formatos para su construcción, utilizando el cifrado estándar mencionado anteriormente TDES (según estándar ISO 9564 – Gestion del PIN).

La norma ISO 9564 menciona que el PIN debe ser cifrado desde la terminal (POS, ATM, PIN PAD) hasta su procesamiento. De igual manera menciona como construir los formatos del PIN BLOCK (formato 0, 1, 2 o 3) y en caso se utiliza cada formato.

De manera a continuación se describen los formatos del PIN Block:

**Formato 0**

El PINBlock se construye mediante un XOR de dos campos de 64 bits: el campo de PIN en texto plano y el campo de número de cuenta, ambos de los cuales comprenden 16 bits de cuatro aperitivos .

**Formato 1**

Este formato debe usarse cuando no está disponible el PAN. El PINBlock se construye concatenando el PIN con un número de transacciones.

**Formato 2**

Es para uso local con sistemas fuera de línea (por ejemplo, sólo las tarjetas inteligentes ). Para esto se debe consultar los requisitos de la Norma ISO 9564 que refiera las condiciones y requisitos a cumplir para la manipulación y la verificación de los PIN que se verifican por una tarjeta inteligente, en lugar de ser enviado al banco para su verificación.

**Formato 3**

Es el mismo que el formato 0, excepto que anexa dígitos con valores aleatorios.

El formato utilizado en las transacciones ATM es el formato 1, el pinblock es conformado y cifrado desde la pin pad para su envío y procesamiento.

## Arquitectura del proyecto

El diagrama de conectividad en producción se muestra en la figura 3.32. Este diagrama fue resultado de la participación de todas las áreas involucradas.

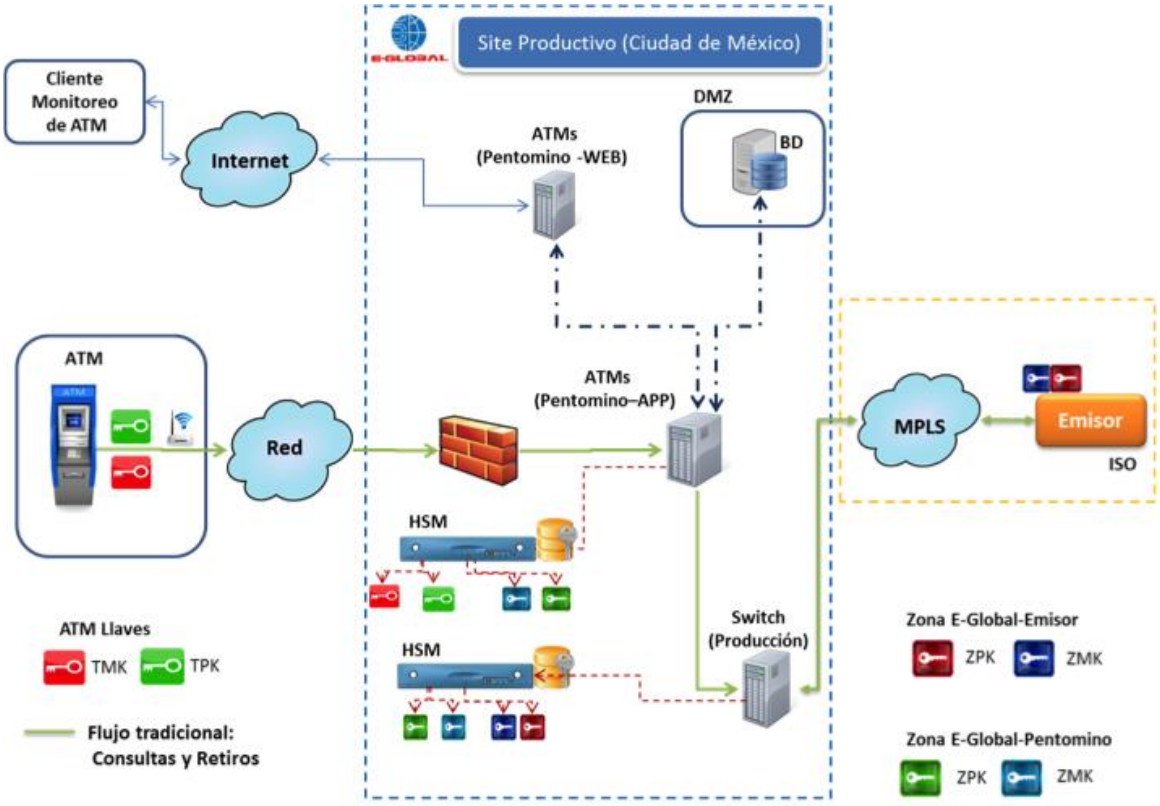



Figura 3.32 Esquema de conectividad

Este diagrama ilustra la arquitectura final del proyecto implementada para brindar el servicio de transacciones de cajeros automáticos, se identifica la conexión de los equipos de cifrado, uno conectado al switch transaccional y otro conectado a la aplicación de Pentomino, también se representa el intercambio de llaves que se describió en la sección anterior. En este diagrama se identifican tres componentes adicionales al servidor PENTOMINO-APP.

- Servidor PENTOMINO-WEB: equipo dedicado al monitoreo de los cajeros automáticos, para identificar las diferentes fallas que puedan presentar e incluso la falta de dinero en los mismos.

- Servidor BD, ubicado en una DMZ, y dedicado almacenar los datos de transacciones realizadas por PENTOMINO y datos de la red de cajeros conectada.

Estos dos componentes adicionales complementa la solución final para la interconexión de cajeros automáticos, y la solución implementada para cifrar TX financieras de cajeros automáticos.

La implementación de la arquitectura inició en septiembre del 2013 y finalizó en agosto del 2014 teniendo una duración de casi un año en desarrollarla y llevarla a cabo.

En la siguiente figura 3.33 se detalla brevemente un cronograma de actividades. La implementación no se logró cubrir de acuerdo a los tiempos definidos a principios de año, ya que se tenía planeado terminar el 2014 con la salida a producción de 25 cajeros de los 50 planteados a inicios del proyecto. Las principales causas del retraso fueron la atención prioritaria de otros proyectos estratégicos de la organización por lo cual la asignación de recursos se vio desfavorecida para este proyecto, sin embargo aun con estas salvedades el proyecto se logró ser implementado para lograr salir a producción para el siguiente año 2015.

| Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin | Predecesoras | Nombres de los recursos |
|---|---|---|---|---|---|---|
| **Infraestructura Front ATM´s** | | **98 días?** | **lun 26/05/14** | **mié 08/10/14** | | |
| | Definición de banco prueba | 5 días | lun 26/05/14 | vie 30/05/14 | | |
| | Cotizaciones, retroalimentaciones con proveedores y el visto bueno hasta que se haga la orden de compra | 21 días | lun 26/05/14 | lun 23/06/14 | | |
| | Adecuaciones físicas y lógicas, Espacio en SITE | 5 días | lun 09/06/14 | vie 13/06/14 | | |
| | Asignación de Ips, cableado de red, reglas de firewalls internos y externos. | 20 días | jue 12/06/14 | mié 09/07/14 | | |
| | Evaluación y configuración de Encriptores | 25 días | lun 16/06/14 | vie 18/07/14 | | |
| | Verifique si el HSM THALES a utilizar para ATM´s ya está depreciado, RN verificara con Alfredo López. | | 27/06/2014 | | | |
| | Verificar si la cuota de mantenimiento seguirá siendo de $8,650 USD más IVA | | 27/06/2014 | | | |
| | Solicitud de IP, puertos y cableado | | 25/06/2014 | | | |
| | Entrega de plan de ejecución de cambio de encriptor Realsec / Thales | | 10 días después de entregado el punto anterior | | | |
| | Cuando se podrá realizar el cambio de encriptor | | TBC | | | |
| | Instalación en producción de HSM | 5 días | lun 21/07/14 | vie 25/07/14 | 21 | |
| | Generacion de llaves de intercambio SWITCH - Pentomino | 15 días | lun 28/07/14 | vie 15/08/14 | 22 | |

Figura 3.33 Bitácora del proyecto

Actualmente esta infraestructura ya opera desde septiembre del 2014 con un par de cajeros, los siguientes pasos son lograr la conexión de 50 cajeros con un par de bancos para el año 2015.

## Resultados

La implementación está concluida y lista para procesar transacciones, las pruebas piloto se han realizado con un par de cajeros en laboratorio y estas han sido satisfactorias, procesando TX de consulta de saldo y retiros. La última prueba de seguridad del esquema de conectividad de la figura 3.33 finalizará con la prueba de PENTEST a nivel de aplicación como a nivel de red, a la conclusión de este trabajo las pruebas de PENTEST están en ejecución, dependiendo del resultado se determinará un tiempo de remediación de las vulnerabilidades que resulten. Estas vulnerabilidades tendrán que ser resultas antes de que el proyecto se libere a producción.

Por otra parte al término de este documento se tiene negociado con dos bancos la puesta en producción de 50 cajeros entre los dos bancos, de continuar sin contratiempos la salida a producción se dará en el primer trimestre del año 2015.

# 5 Conclusiones

### Conclusiones del proyecto

El alcance principal en estas tres fases es contar con un ambiente de desarrollo y uno de producción implementados para la integración de una red de cajeros automáticos, las actividades realizadas por el equipo de trabajo se enfocaron en definir sus diversos requerimientos y controles de acuerdo a cada ámbito de responsabilidad, el área de seguridad de la información logró implementar una arquitectura robusta y segura que consigue brindar el servicio de red de cajeros automáticos con controles que garanticen el cumplimiento de normas internacionales, así como la disponibilidad, confidencialidad e integridad de la información del servicio que se espera ofrecer. En este sentido los logros alcanzados son dos principalmente:

- Implementar una infraestructura de desarrollo para la integración de nuevos clientes a la red de cajeros.
- Implementar una infraestructura que brinde la inter-conexión de cajeros automáticos a nivel nacional ofreciendo seguridad, disponibilidad y confianza en el servicio a un bajo costo.

Con estos dos logros alcanzados la empresa consigue tener un servicio adicional que puede ofrecer, y el cual puede ser ofrecido a clientes actuales. Teniendo como plus adicional un servicio más dentro de nuestra cartera de productos para lograr la atracción de nuevos clientes.

El crecimiento del producto se vislumbra de manera positiva ya que se contempla la inter-conexión de 50 cajeros automáticos para el primer semestre del año 2015, con esta implementación E-Global estaría ingresando a un nicho del mercado que solo era ofrecido por una sola empresa en México.

Durante el desarrollo y documentación de este proyecto se definieron diversas actividades en diferentes ámbitos de responsabilidad, en lo que compete al área de seguridad de la información las actividades realizadas como: la arquitectura de cifrado implementada, establecer el esquema de intercambio de llaves conforme a las normas internacionales y la definición de controles de seguridad en diversos puntos, fueron actividades que me dejaron un gran aprendizaje. Y en este sentido los logros alcanzados fueron satisfactorios consiguiendo implementar en una primer fase todo el modelo para una arquitectura de desarrollo reduciendo los costos, re-utilizando infraestructura y equipos que no estaban en uso. Logrando reducir costos de implementación, alcanzando un esquema de desarrollo suficiente para realizar pruebas de integración y validación para clientes futuros que deseen tener el servicio de la red de cajeros.

La implementación de la arquitectura para la puesta en producción se realizó algunas modificaciones con la finalidad de robustecer los controles de seguridad de tal manera que se garanticen la disponibilidad, confidencialidad e integridad en el servicio pero sin afectar costos y tiempos.

Se aprovechó la sustitución de los equipos de cifrado de producción los cuales brindaban otros servicios, esto ayudó a que los costos del proyecto se mantengan conforme a lo planeado y los tiempos de instalación no se vean modificados drásticamente, el proyecto pudo avanzar hasta tener una arquitectura de cifrado robusta que garantice el servicio.

Por último, se estableció el esquema de intercambio y gestión de las llaves de cifrado, teniendo una participación como custodio y responsable principal de las llaves y elementos de cifrado de la organización. La ejecución de las pruebas y la validación en el intercambio de llaves fue una tarea que llevo tiempo en estudio y análisis de traslado y transporte de la información, siendo para mí un tema nuevo desde las definiciones de generación e intercambio de llaves. En términos generales los objetivos planteados en fase I y fase II se lograron satisfactoriamente.

## Conclusiones personales

De manera personal me siento satisfecho con mi participación, fue un proyecto que implicó una serie de retos en todos los sentidos desde el ámbito profesional hasta el ámbito meramente social y humano, implicando un reto la coordinación e interacción con las personas que trabajaron en este proyecto. Sin duda lo que queda al final del proyecto son los logros y conocimiento adquirido, pero las experiencias y las relaciones o lazos que uno pueda formar con las personas en la convivencia diaria es un logro que uno se puede llevar con más satisfacción, y en la medida que se tenga la oportunidad de ayudar y aportar para que los compañeros del equipo crezcan es lo que hace a uno crecer como ser humano y no solo en el ámbito laboral.

Sin duda el desarrollo académico que brinda la Facultad de Ingeniería ha sido importante para el desempeño de mis funciones en el trabajo. Los conocimientos que adquirí durante la carrera profesional han sido la base para llevar a cabo el trabajo que se me asigna, la formación académica que brinda ayuda a generar habilidades de razonamiento, análisis, autoestudio y trabajo en equipo, que son indispensables en las actividades dentro de una organización. En mi corta experiencia laboral he podido aplicar los conocimientos adquiridos durante la carrera profesional y he seguido aprendiendo gracias a los retos profesionales como este proyecto. Las metas propuestas, el estudio constante, mantenerme informado y actualizado han sido base fundamental para continuar desempeñando las actividades del trabajo lo mejor posible.

Al concluir el proyecto lo que me puedo llevar son las amistades y lazos que alcancé a forjar así como la satisfacción de aplicar los conocimientos que adquiridos durante la trayectoria académica y profesional.

# 6 Glosario de términos

## A

**Amenaza**
Hecho que puede producir un daño provocado por un evento natural o de índole humano, que ponga en riesgo la estabilidad de un sistema o ambiente.

**Análisis de riesgos**
Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

**Análisis de vulnerabilidades**
Es un método sistemático utilizado para evaluar y registrar las posibles brechas de seguridad que existe en un sistema o ambiente y que pongan en riesgo la estabilidad del mismo.

**Arquitectura de red**
Es el diseño de una red de comunicaciones, indica los componentes físicos y especificaciones de una red sus principios de operación y procedimientos en una organización.

**Arquitectura de seguridad**
Son las definiciones y prácticas que se deciden adoptar por parte de una organización a los procesos, gente y tecnología que garanticen la disponibilidad, confidencialidad e integridad de la información.

## B

**Buenas prácticas**
Traducción literal del término en inglés *best practices,* y se refieren al conjunto de acciones coherentes recomendadas por organismos internacionales para llevar acabo y garantizar ciertos estándares de calidad, seguridad y servicio.

**Base de datos**
Se refiera al conjunto de datos almacenados sistemáticamente y bajo un mismo contexto.

## C

**Continuidad del negocio**
Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

**Confidencialidad**
Es una propiedad de la información, la cual garantiza que sea accesible únicamente por personal autorizado.

**Cambio no autorizado**
Solicitud realizada para ejecutar algún tipo de configuración en un sistema o ambiente y el cual no fue aprobado para su aplicación por el comité de cambios o las personas facultadas.

**Cambio emergente**
Solicitud realizada para ejecutar algún tipo de configuración en un sistema o ambiente y el cual fue necesario realizar en instante para corregir algún problema o falla en el sistema, obteniendo la aprobación posterior del comité de cambios o las personas facultadas.

**Coercitividad**
También llamada campo coercitivo o fuerza coercitiva de un material ferromagnético es la intensidad del campo magnético que se debe aplicar a un material para reducir su magnetización a cero. La coercitividad mide la resistencia de un material ferromagnético a ser desmagnetizado.

# D

**Disponibilidad**
Medida que nos indica cuánto tiempo está un equipo o sistema operativo en servicio o funcionando respecto de la duración total durante la que se hubiese deseado que funcionase.

**Datos en transito**
Se refiera a la información que viaje por un medio lógico comúnmente llamado enlace, este enlace trasmite información o datos.

**Datos almacenados**
Conjuntos de datos resguardados en un repositorio, comúnmente en una base de datos.

# E

**Estándares**
Protocolo o técnica empleada para ejecutar un proceso o actividad de una manera correcta.

**Evidencia**
Material o conocimiento significativo que define la existencia o certeza de un hecho.

**Escaneo de vulnerabilidades**
Actividad que se realiza para identificar posibles brechas de seguridad en infraestructura de TI (hardware o software).

**Explotación de vulnerabilidades**
Actividad que aprovecha las brechas o bondades que existen en los sistemas para ejecutar acciones que de manera formal no serían permitidas.

# G

**Gestion de hallazgos**
Se refiera a la actividad que se realiza para atender una brecha, incidente o vulnerabilidad de seguridad, desde su identificación, seguimiento, atención y cierre.

**Gestion de llaves**
Se refiera a la actividad que se realiza para dar tratamiento a los elementos de cifrado desde su generación hasta su resguardo o eliminación.

# H

**Hallazgo**
Descubrimiento, acción de hallar o encontrar una cosa u objeto.

# I

**Integridad**
Bajo el contexto de seguridad nos referimos como una propiedad de la información por conservar su estado original de creación, al sufrir modificaciones o alteraciones y perder su estado original se dice que se la información perdió su integridad.

**Información**
Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

**IPSEC**
Abreviatura de Internet Protocol security, un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

# L

**Logs**
Término anglosajón, equivalente a la palabra bitácora en español.

# M

**Marco normativo**
Conjunto general de normas, criterios, metodologías, lineamientos y sistemas, que establecen la forma en que deben desarrollarse las acciones para alcanzar los objetivos de la organización.
**Medios de pagos**
Un activo que se puede usar como dinero como forma de pago.

**Metodología**
Conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos

**MPLS**
Multiprotocol Label Switching, mecanismos de transporte de datos. Utilizada para la transmisión de diferente tipo de datos.

# P

**Pentest – Prueba de intrusión**
Se define como un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad, lo que podría tener acceso a ella, su funcionalidad y los datos.

**Políticas**
En el sentido de una organización o empresa, se refiere al conjunto de normas que rigen a una institución y la cual empleados y colaboradores deben seguir.

**Procedimiento**
Es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias

**Procesamiento Batch**
Procesos operativos aplicados en una ventana de tiempo durante periodos programados. En el ámbito que nos compete se refieren a proceso de transacciones financieras (compras, cargos, abonos, traspasos, etc.) que se aplican en ventanas de tiempo programas con cierta periodicidad

**Procesamiento en línea**
Procesos operativos que se ejecutan en el mismo instante de tiempo, a diferencia de un procesamiento batch las transacciones financieras se ejecutan en el instante que son solicitadas, por ejemplo: retiro de efectivo, compra, traspaso de dinero del mismo banco, por mencionar algunos.

# S

**Security Awareness**
Término utilizado en el ámbito de seguridad de la información para referirse al programa de capacitación y concientización de las personas en temas de seguridad, con la finalidad es difundir una cultura de prevención en delitos, fraudes y robo de información de las personas.

# T

**Tecnologia**
Es el conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar y crear bienes.

# V

**VPN**
Red Privada Virtual, permite a dispositivo de red comunicarse a través de redes públicas a una red local de trabajo o privada

**Vulnerabilidad**
En términos de seguridad son puntos débiles del software o hardware que permiten a un atacante comprometer la integridad, disponibilidad o confidencialidad del mismo.

# 7 Fuentes de Información

| Direcciones web - URL | Fecha de consulta |
|---|---|
| http://mx.selecciones.com/contenido/a2706_como-funcionan-los-cajeros-automaticos | 25/06/2014 |
| http://www.delitosinformaticos.com/06/2013//fraudes/fraude-en-cajeros-automaticos-consejos-de-seguridad#.U6O_2PldX2Y | 25/06/2014 |
| http://windows.microsoft.com/es-xl/windows/what-is-encryption#1TC=windows-7 | 25/06/2014 |
| http://highsec.es/2014/01/criptografia-parte-i-conceptos-basicos/ | 25/06/2014 |
| http://es.kioskea.net/contents/129-criptografia | 25/06/2014 |
| http://www.math.com.mx/criptografia.html | 30/06/2014 |
| https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/c/block_encryption.htm | 9/07/2014 |
| http://computacion.cs.cinvestav.mx/~jjangel/aes/AES_v2005_jjaa.pdf | 9/07/2014 |
| http://es.scribd.com/doc/119961571/Algoritmos-de-Cifrado-Moderno | 9/07/2014 |
| http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/4-criptografia-simetrica-o-de-clave-secreta/43-aes-advanced-encryption-standard/431-origenes | 9/07/2014 |
| http://es.wikipedia.org/wiki/Cifrado_por_bloques | 9/07/2014 |
| http://www.edukanda.es/mediatecaweb/data/zip/638/PID_00150197/web/main/m3/v3_2_2.html | 9/07/2014 |
| http://gaussianos.com/%C2%BFque-significan-los-numeros-de-nuestra-tarjeta-de-credito/ | 15/07/2014 |
| http://es.wikipedia.org/wiki/Cifrador_de_flujo | 15/07/2014 |
| http://cala.unex.es/cala/epistemowikia/index.php?title=Codificaci%C3%B3n | 15/07/2014 |
| http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/ | 15/07/2014 |
| http://www.publispain.com/supertutoriales/matematica/criptografia/cursos/2/curva.pdf | 17/07/2014 |
| http://portalae.sci.uma.es:8080/export/sites/default/uma/documentos/criptografia_certificado_digital_firma_digital.pdf | 17/07/2014 |
| http://www.ecured.cu/index.php/MD5 17/05/2014 | 17/07/2014 |
| http://technologyincontrol2.wordpress.com/2014/01/03/criptografia-y-proteccion-de-datos-1-de-2/ | 22/07/2014 |
| http://technologyincontrol2.wordpress.com/2014/01/20/criptografia-y-proteccion-de-datos-2-de-2/ | 22/07/2014 |
| http://www.redbanc.cl/portal_redbanc/browse?pagina=portal_redbanc/inicio.htm | 1/08/2014 |
| http://www.bancafacil.cl/bancafacil/servlet/Contenido?indice=1.2&idPublicacion=3000000000000023&idCategoria=6 | 1/08/2014 |
| http://www.unla.mx/iusunla14/actualidad/CAJEROS%20AUTOMATICOS.htm | 1/08/2014 |
| http://codigopgt.wordpress.com/2008/03/05/como-funciona-un-cajero-automatico/ | 1/08/2014 |
| http://centrodeartigos.com/articulos-utiles/article_111104.html | 1/08/2014 |

| | |
|---|---|
| http://nosoloingenieria.com/como-funciona-tarjetas-banda-magnetica/ | 14/08/2014 |
| http://es.wikipedia.org/wiki/Tarjeta_de_cr%C3%A9dito | 14/08/2014 |
| http://gaussianos.com/%C2%BFque-significan-los-numeros-de-nuestra-tarjeta-de-credito/ | 14/08/2014 |
| http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica2.shtml | 14/08/2014 |
| http://gaussianos.com/%C2%BFque-significan-los-numeros-de-nuestra-tarjeta-de-credito/ | 14/08/2014 |
| http://www.monografias.com/trabajos43/banda-magnetica/banda-magnetica2.shtml | 14/08/2014 |
| http://es.wikipedia.org/wiki/Tarjeta_de_cr%C3%A9dito | 14/08/2014 |
| http://nosoloingenieria.com/como-funciona-tarjetas-banda-magnetica/ | 14/08/2014 |
| http://www.banxico.org.mx/ | 29/01/2014<br>14/08/2014 |
| http://en.wikipedia.org/wiki/ISO_9564 | 13/10/2014 |

| Documentos PDF consultados | Fecha de consulta |
|---|---|
| NORMA ISO 27000 2000:2005 | 7/04/2014 |
| ACUERDO INTERBANCARIO SEGURIDADES FÍSICAS Y DE LA INFORMACIÓN PARA CAJEROS AUTOMÁTICOS, PUNTOS DE VENTA, Y TARJETAS DE CRÉDITO Y DÉBITO, ASOCIACIÓN BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA Bogotá, D.C. Junio de 2006 | 7/04/2014 |
| FUNDACIÓN DE ESTUDIOS FINANCIEROS - México | 10/05/2014 |
| Seguridad criptográfica Normativa de Seguridad Documental del Sector Público de Cataluña. | 10/05/2014 |
| UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL (UCI) - PROPUESTA DE UN PLAN PARA ADQUIRIR UNA SOLUCION TECNOLOGICA QUE PERMITA LA ADMINISTRACION Y MONITOREO DE LA RED DE CAJEROS AUTOMATICOS DEL BANCO POPULAR Y DE DESARROLLO COMUNAL - San José, Costa Rica JUNIO, 2009 | 15/06/2014 |
| Descripción de las Tasas de Descuento y Cuotas de Intercambio en el pago con tarjetas bancarias en México | 15/062014 |
| Diseño del sistema de tarjeta de crédito con UML – Tesis digitales, central UNMSM | 15/062/014 |