Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Controles de seguridad de información para las claves criptográficas de ATMs del Banco de la Nación usando el estándar EMV

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Jesús Nieves QUEVEDO URIBE

ASESOR

José Antonio PÉREZ QUINTANILLA

Lima, Perú

2008

Referencia bibliográfica

Quevedo, J. (2008). *Controles de seguridad de información para las claves criptográficas de ATMs del Banco de la Nación usando el estándar EMV*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Dedico el presente trabajo a mi mamá, por su amor y fortaleza, que ha sido mi inspiración.

AGRADECIMIENTOS

Al profesor José Antonio Pérez Quintanilla, por su orientación y dedicación para que este trabajo cumpla con los objetivos trazados.

Al profesor David Mauricio Sánchez, por las pautas metodológicas para la elaboración de este trabajo.

A mis hermanos Fiorella, Natalia y Orlando, por su alegría y apoyo.

A mi tía Maritza, por sus cuidados y ánimo.

A mi mejor amigo Segundo, por su apoyo y por todo el conocimiento aportado en criptografía y seguridad de información.

A la División Seguridad de Información del Banco de la Nación, por la formación profesional y oportunidades brindadas.

A la Facultad de Ingeniería de Sistemas – UNMSM, por la formación académica brindada durante los cinco años de estudios.

A Dios.

Controles de Seguridad de Información para las claves criptográficas de ATMs del Banco de la Nación usando el estándar EMV

RESUMEN

Las tarjetas de banda magnética están siendo el objetivo de constantes ataques a su seguridad, no sólo por la debilidad de los controles tecnológicos e informáticos en sí, sino de administración de dichos controles a nivel organizacional.

Este trabajo busca definir controles de seguridad para la administración interna de las claves criptográficas usadas para encriptar la información que viaja en transacciones de cajeros automáticos del Banco de la Nación, considerando una migración del algoritmo DES al estándar EMV, por lo tanto, el uso de tarjetas inteligentes en reemplazo de las tarjetas de banda magnética.

Palabras Claves: control, información, seguridad, criptografía, ATM, tarjeta.

Information Security Controls for ATM's cryptographic keys of The National Bank using EMV standard

ABSTRACT

Magnetic-strip cards are being target of continuous attacks against their security, not only because of the weakness of the technologic and informatics controls, also the management of those controls in organizational level.

This work tries to define security controls for internal management of cryptographic keys used to encrypt the information that travels in automatic-teller-machine transactions of The National Bank, considering a migration from DES algorithm to EMV standard, what means, the smart cards use instead of magnetic stripe cards.

Key words: control, information, security, cryptography, ATM, card.

ÍNDICE

Lista de Figuras vi

Lista de Tablas vii

Capítulo 1: Introducción *1*

1.1 Antecedentes **2**

1.1.1 Seguridad de Información 2

1.1.2 Criptografía 4

1.1.3 Tarjetas de Banda Magnética 7

1.1.4 Tarjetas Inteligentes 9

1.1.5 Fraude en Cajeros Automáticos 10

1.1.6 Franquicias 13

1.1.7 Tarjetas Multired Global Débito 14

1.2 Definición del Problema **14**

1.3 Objetivos **15**

1.3.1 General 15

1.3.2 Específicos 16

1.4 Justificación **16**

1.5 Propuesta **17**

1.6 Organización de la Tesina **18**

Capítulo 2: Marco Teórico *19*

2.1 Definiciones Teóricas **19**

2.1.1 Confidencialidad 19

2.1.2 Integridad 19

2.1.3 Disponibilidad 20

2.1.4 Autentificación 20

2.1.5 No-Repudio 20

2.1.6 Continuidad del servicio 21

2.1.7 Evaluación de Riesgos 22

2.1.8 Conceptos de Sistemas de Pagos 22

2.1.9 Llaves Criptográficas 24

2.1.10 El Algoritmo DES 29

2.1.11 Algoritmos asimétricos 33

2.1.12 Public Key Infrastructure (PKI) 34
a. Firma digital 35
b. Certificados digitales 36
c. Autoridad Certificadora 38
d. Proceso de Firma 38
2.1.13 Banda Magnética 39
2.1.14 Tarjetas Inteligentes 40
a. Ventajas: 41
b. Clases de tarjetas inteligentes 42
c. ISO 7816 43
2.1.15 El Estándar EMV (EUROPAY, MASTERCARD AND VISA) 45
2.1.16 Módulo de Seguridad Resistente a Alteraciones 48
FIPS PUB 140-1 Security Requirements for Cryptographic Modules 50
FIPS PUB 140-2 Cryptographic Module Validation Program (CMVP) 51
2.1.17 Cajero Automático 51

2.2 Marco Conceptual 52

Capítulo 3: Estado del Arte 56

3.1 Taxonomía de algoritmos criptográficos 56
3.1.1 Características técnicas 56
3.1.2 Uso típico 57
3.1.3 Estado comercial o legal 59
3.1.4 Dominio de Aplicación 60

3.2 Estructura de Llaves Criptográficas del Banco de la Nación 61
3.2.1 Llave Maestra – Local Master Key (LMK) 61
3.2.2 Llaves de Encripción de Llaves – Key Encrypting Key (KEK) 62
3.2.2.1 Zone Master Key (ZMK) 62
3.2.2.2 Terminal Master Key (TMK) 63
3.2.3 Llaves de Trabajo – Working Key 64
3.2.3.1 Card Verification Key (CVK) 64
3.2.3.2 PIN Verification Key (PVK) 65
3.2.3.3 Zone PIN Key (ZPK) 66
3.2.3.4 Terminal PIN Key (TPK) 67
3.2.3.5 Message Authentication Code (MAC) 68
3.2.4 Valor de Chequeo 69
3.2.5 PIN Block 69
3.2.6 Esquema de validación actual 69

3.3 Host Security Module HSM 8000 74
3.3.1 Seguridad Física 74

3.4 Organización del Banco de la Nación 75

3.4.1 División Seguridad de Información 76

3.4.2 Sección Procesamiento Central 77

3.4.3 Administrador de Agencia (Oficina de Respaldo) 77

3.4.4 Administradores de Agencias de Provincias 78

3.4.5 Jefes de Operaciones de Provincias 78

3.4.6 Sección Instalaciones y Configuraciones 78

3.4.7 Sección Canales Virtuales 79

3.4.8 Sección Canales Remotos 79

3.4.9 Gerentes de Departamento 79

3.4.10 Departamento de Planeamiento y Desarrollo 79

3.4.11 Gerencia General 79

3.5 Estándar EMV 80

3.5.1 Autenticación Offline Estática de Datos 80

3.5.2 Autenticación Offline Dinámica de Datos 81

3.5.3 Cifrado del PIN offline 83

3.5.4 Principios de Administración de llaves y tipos de llaves criptográficas para tarjetas de circuito integrado (Integrated Circuit Card ICC) 84

3.5.4.1 Administración de llaves asimétricas (RSA) 84

3.5.4.2 Administración de Llaves Simétricas 89

3.5.4.3 Generación de Llaves – Guía General 93

3.5.4.4 Custodia de Llaves – Prácticas y Responsabilidades 94

3.5.4.5 Equipos Criptográficamente Seguros (Secure Cryptographic Devices SCD) 96

3.5.4.6 El Sistema de Autorización 99

3.5.4.7 Seguridad de la Aplicación de la Tarjeta IC 100

3.5.4.8 Detección de Fraude 102

Capítulo 4: Análisis de Riesgos 104

4.1 De la evaluación de riesgos 104

4.2 De las Claves Criptográficas electrónicas 105

4.2.1 Generación 105

4.2.2 Segregación 107

4.2.3 Reemplazo 107

4.2.4 Transporte 108

4.2.5 Destrucción 108

4.2.6 Almacenamiento 109

4.2.7 Respaldo 110

4.2.8 Custodia 110

4.3 De las Claves Criptográficas en papel 111

4.3.1 Generación 111
4.3.2 Reemplazo 112
4.3.3 Transporte 113
4.3.4 Destrucción 113
4.3.5 Almacenamiento 113
4.3.6 Respaldo 114
4.3.7 Custodia 114

4.4 Del Coprocesador Criptográfico 115
4.4.1 De la Generación de llaves 115
4.4.2 De la restauración 116

4.5 De la Banda Magnética 116

4.6 Del Algoritmo DES 116

4.7 De los HSM 116

4.8 De la grabación de tarjetas 117

4.9 De la operación 118

Capítulo 5: Controles de seguridad de información para las claves criptográficas de los ATMs del Banco de la Nación 119

5.1 De las Claves Criptográficas 119
5.1.1 Generación 119
5.1.2 Segregación 123
5.1.3 Reemplazo 123
5.1.4 Transporte 124
5.1.5 Destrucción 125
5.1.6 Almacenamiento 129
5.1.7 Respaldo 129
5.1.8 Custodia 130
5.1.9 De la Operación 132

5.2 De las Claves Criptográficas en papel 134
5.2.1 Generación 134
5.2.2 Reemplazo 135
5.2.3 Transporte 136
5.2.4 Destrucción 136
5.2.5 Almacenamiento 136
5.2.6 Respaldo 137
5.2.7 Custodia 138

5.3 Del Coprocesador Criptográfico 138

5.4 De los HSM 139
5.4.1 Seguridad física 139
5.4.2 Seguridad lógica 140
5.5 Grabación de tarjetas 141
5.5.1 Seguridad Física 141
5.5.2 Seguridad lógica 143
5.5.3 Procesamiento 144
5.6 De la operación 145
5.6.1 Procesamiento de la información 145
5.6.2 Flujo de instalación de llaves desde los HSM a los ATM 146
5.6.3 Transacciones en ATMs del Banco de la Nación 147
5.6.3.1 Transacciones On-US – Rol Emisor 147
5.6.3.2 Transacciones Domésticas – Rol Adquirente 147
5.6.3.3 Transacciones Internacionales – Rol Adquirente 148
5.6.4 Transacciones en ATMs de otros bancos 148
5.6.4.1 Transacciones Domésticas – Rol Emisor 149
5.6.4.2 Transacciones Internacionales – Rol Emisor 149
5.6.5 Flujo de aceptación de operaciones de una tarjeta chip en un ATM 150
Capítulo 6: Conclusiones y trabajos futuros 154
6.1 Conclusiones 154
6.2 Trabajos Futuros 155
Capítulo 7: Glosario de Términos 156
Capítulo 8: Referencias Bibliográficas 158

Lista de figuras

1.1 Entorno de la Seguridad de Información 03

1.2 Ejemplo de clave de sustitución 06

1.3 Ejemplo de clave de transposición 07

1.4 Ejemplo de clave en bloque 07

2.1 Esquema de interconexión de entidades 24

2.2 Modelo de encriptación/desencriptación con claves simétricas 27

2.3 Modelo de encriptación/desencriptación con claves asimétricas 28

2.4 Esquema de la función f del algoritmo DES 30

2.5 Cálculo de las K_i para el algoritmo DES 32

2.6 Transmisión de información empleando algoritmos asimétricos 33

2.7 Autentificación de información empleando algoritmos asimétricos 34

2.8 Generación de Certificados digitales 38

2.9 Composición de la Pista 1 40

2.10 Composición de la Pista 2 40

2.11 Tarjeta Inteligente Visa 41

2.12 Esquemas de Tarjetas Asíncronas 43

2.13 Composición interna de tarjetas Chip 48

2.14 HSM 8000 49

3.1 Una taxonomía técnica de primitivas y mecanismos criptográficos 57

3.2. Carga de componentes en cada ATM 64

3.3 Esquema de generación de CVV 65

3.4 Esquema de generación de PVV 66

3.5 Relación entre las llaves ZMK y ZPK 67

3.6 Relación entre las llaves TMK y TPK 68

3.7 Relación de ZMK, TMK, Adquirente y Emisor 69

3.8 Esquema de conexión interna actual 70

3.9 Organigrama del Banco de la Nación 76

5.1 Acta de Generación de Llaves 121

5.2. Acta de Destrucción de Componentes 129

5.3 Acta de Custodia 131

5.4 Bitácora de Accesos a la Consola de Administración de los HSM 134

5.5 Bitácora de Accesos a la Caja Fuerte 137

5.6 Acta de Destrucción de Tarjetas 145

Lista de tablas

1.1 Estadísticas del uso de tarjetas a nivel mundial 08

1.2 Comparación de DES y EMV 17

2.1 Operación lógica XOR 31

3.1 Comparación de técnicas y funcionalidades de seguridad 58

3.2. Datos de composición del CVV 65

3.3 Estados posibles del HSM 8000 según llaves físicas 75

3.4 Tamaño de llaves EMV y criptoperíodos 85

4.1. Nivel de Criticidad de Riesgos 104

5.1 Comandos de diagnóstico del HSM 8000 120

5.2 Comandos de configuración de seguridad del HSM 8000 126

5.3 Comandos de visibilidad de LMK del HSM 8000 127

5.3 Comandos de formateo de tarjetas del HSM 8000 128

5.4 Comandos de configuración de alarmas del HSM 8000 139

Capítulo 1: Introducción

Hasta ahora, la banda magnética de las tarjetas de crédito y de débito ha sido la tecnología dominante en el mercado; sin embargo, en ellas sólo se puede almacenar una pequeña cantidad de información, de modo que la gran mayoría de los datos personales y de las operaciones de la tarjeta de banda magnética, residen en servidores centrales de la compañía que las emite. De manera paralela, esta tecnología ha ido perdiendo fiabilidad al encontrarse más vulnerabilidades tanto en el envío de la información, como los algoritmos usados y la facilidad de clonación.

Gracias al enorme progreso de la microelectrónica desde los años setenta, se hizo posible el almacenamiento de datos en chips de silicio de tamaño considerablemente reducido. En los últimos años, el manejo masivo de información sensible ha permitido el desarrollo y mejora sustancial en las aplicaciones y protocolos de seguridad para las tarjetas que utilizan circuitos integrados, ya que permiten acceso seguro y autenticado de usuarios a sistemas y redes. Con la inclusión de estas tarjetas en la Sociedad de la Información, es necesario implementar mecanismos para el uso de datos personales, que permitan su protección a un nivel aceptable.

La seguridad que brindan las tarjetas inteligentes se basa en el uso de algoritmos criptográficos más robustos que los usados actualmente por las tarjetas de banda magnética. El algoritmo asimétrico RSA (Rivest, Shamir y Adleman, apellidos de sus creadores) es el que se considera actualmente como una de las modalidades más seguras del mercado. Utilizado también en la Infraestructura de Llave Pública o PKI (Public Key Infrastructure), el algoritmo RSA está basado en el uso de un par de llaves asimétricas, una pública y otra privada, por cada entidad. La Llave Privada debe permanecer en secreto y bajo el control del usuario. La Llave Pública puede y debe ser libremente distribuida.

Para reforzar el proceso de encripción y desencripción, los equipos de seguridad HSM (Host Security Module) soportan los esquemas de llaves simétricas y asimétricas y

brindan un nivel adicional de seguridad al ser equipos que cumplen con estándares internacionales tales como FIPS (Federal Information Processing Standard) y EMV (Europay, MasterCard and Visa).

Pero a pesar de todos estos controles tecnológicos, aún existe una brecha de seguridad importante. La experiencia de las empresas en la implementación de sistemas y controles de seguridad de información determina que el eslabón más débil y más difícil de controlar en la cadena de la seguridad de información son las personas. 'Los empleados descontentos pueden significar una pérdida de datos causada por robo de identidades, violación de normas o daño a la imagen pública de una organización. Las nuevas leyes de divulgación permiten que el público actualmente tenga más conocimiento sobre las violaciones de seguridad que en el pasado, incluyendo aquellas causadas por personal interno.' [Jones08B]

De la misma manera, para la criptografía, el parámetro que genera más riesgos es la administración de las claves criptográficas ya que se encuentra bajo la responsabilidad del personal de la empresa. Es por ello que los controles para administración de dichas claves criptográficas es el objetivo de este trabajo.

1.1 Antecedentes

1.1.1 Seguridad de Información

Los activos de información existen en un ecosistema multifacético y complejo de procesos empresariales, tecnologías, requisitos regulatorios, presiones de mercado y, por supuesto, amenazas de seguridad. La información se mueve mediante flujos de trabajo elaborados a través de aplicaciones integradas y respaldadas por un arreglo de redes, bases de datos, mensajería y servidores de colaboración y de aplicaciones, para cumplir con los objetivos del negocio. Las entidades reguladoras (tales como SBS, INDECOPI, PCM y otras) determinan las barreras de cómo y donde fluye la información, así como el nivel de calidad de los datos y precisión de la información que se ha de brindar a los usuarios.

Simultáneamente, las empresas deben responder a las exigencias del mercado para disminuir costos, mejorar servicios e innovar productos. La capacidad de apoyar aplicaciones de negocio integradas e integrales, responder al mercado y cumplir con las regulaciones nacionales e internacionales representa un equilibrio desafiante. La introducción de la constante amenaza hacia la seguridad hace que el equilibrio sea aún más complejo [Jones08A]. Una estrategia integral de administración de información es esencial para perdurar en el contexto actual de información, según nos muestra la figura 1.1:

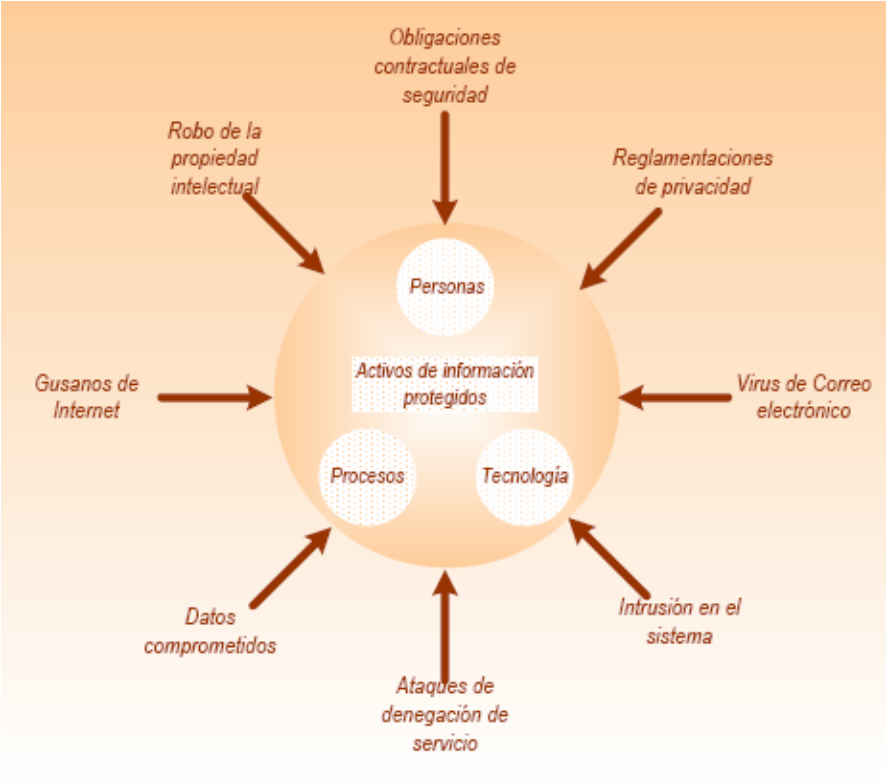


Figura 1.1. Entorno de la Seguridad de Información [Jones08A]

Desde el siglo pasado, hemos podido observar el importante nivel de evolución y uso de las tecnologías de información y el volumen de información digital gestionada a nivel mundial, siendo estos factores respaldados por las grandes inversiones que las instituciones públicas y privadas realizan con el objeto de mejorar los servicios y obtener grandes beneficios.

Sin embargo, como consecuencia también podemos apreciar el incremento de las amenazas contra la seguridad que afectan a la información y a las

comunicaciones. Estas amenazas pueden quebrar la estructura de seguridad en cualquiera de sus planos, que se traducen más allá de su incidencia individual en considerables pérdidas económicas para las organizaciones. De esta manera, se ven forzadas a identificar, atender y gestionar los, cada vez más frecuentes, incidentes de seguridad [Torres06].

Es por ello que se presenta la necesidad de implantación de medidas de prevención y protección, la cual es cada vez mejor identificada por la alta dirección y plasmada en sus respectivos Sistemas de Gestión de Seguridad de Información SGSI; teniendo en cuenta que el establecimiento de estas medidas no elimina la posibilidad de que dichos incidentes se produzcan, pero si permite limitarlos y mantenerlos en un nivel de riesgo que puede ser asumido por la organización.

La seguridad de información puede entenderse como la consecución de un conjunto de determinados servicios de seguridad, de los que puede extraerse como fundamentales: la confidencialidad, la integridad, la disponibilidad y la autenticación [Torres06].

1.1.2 Criptografía

La Criptografía moderna nace al mismo tiempo que las computadoras. Durante la Segunda Guerra Mundial, en un lugar llamado Bletchley Park, un grupo de científicos entre los que se encontraba Alan Turing, trabajaba en un proyecto llamado ULTRA, que trataba descifrar los mensajes enviados por el ejército alemán con el más sofisticado ingenio de codificación ideado hasta entonces: la máquina Enigma. Este grupo de científicos empleaba el que hoy se considera el primer computador, una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la

criptografía como en el del criptoanálisis no empezaron hasta entonces. [Güimack07]

Su uso y la llegada del polaco Marian Rejewski tras la invasión de su país natal, cambiarían para siempre el curso de la Historia.

También se desarrolló el proceso criptográfico llamado 'Lucifer' por el Watson Research Laboratory de IBM a principios de la década de los setenta. Este algoritmo se puso a disposición del American National Standards Institute (ANSI) libre del pago de regalías. Después de pasar por algunas modificaciones y un análisis a fondo por parte de varias agencias de seguridad, este algoritmo, actualmente conocido como Data Encryption Standard (DES) en la publicación ANSI X3.92, se estableció como el único método aceptable para proteger el Número de Identificación Personal o PIN (Personal Identification Number) durante la transmisión de los datos del portador de la tarjeta (llamado a partir de aquí 'tarjetahabiente') y la cuenta a través de las redes electrónicas del sistema de pago en los Estados Unidos.

Desde entonces hasta hoy ha habido un crecimiento espectacular de la tecnología criptográfica, si bien la mayor parte de estos avances se mantenían y se siguen manteniendo, según algunos en secreto. Financiadas fundamentalmente por la NSA (Agencia Nacional de Seguridad de los Estados Unidos), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares. Sin embargo en los últimos años, investigaciones serias llevadas a cabo en universidades de todo el mundo han logrado que la criptografía sea una ciencia al alcance de todos, y que se convierta en la piedra angular de asuntos tan importantes como el comercio en Internet. [Visa02]

Muchas son las voces que claman por la disponibilidad pública de la criptografía. La experiencia ha demostrado que la única manera de tener buenos

algoritmos es que éstos sean públicos, para que puedan ser sometidos al escrutinio de toda la comunidad científica. Casos claros de oscurantismo y de sus nefastas consecuencias han sido la caída del algoritmo que emplean los teléfonos GSM en menos de cuarenta y ocho horas desde que su código fue descubierto. Además se puso en evidencia la deliberada debilitación del algoritmo que los gobiernos habían impuesto a sus creadores para facilitar las escuchas por parte de sus servicios de espionaje. Otro ejemplo son los graves problemas de seguridad que presentaba el protocolo de comunicaciones seguras punto a punto que Microsoft incluía en Windows NT. La seguridad no debe basarse en mantener los algoritmos ocultos, puesto que éstos, tarde o temprano, acaban siendo analizados y descritos, sino en su resistencia demostrada tanto teórica como prácticamente, y la única manera de demostrar la fortaleza de un algoritmo es sometiéndolo a todo tipo de ataques. [Lucena99]

Con anterioridad al desarrollo y adopción de los métodos criptográficos utilizados en el presente, la información confidencial estaba mayormente protegida por algún tipo de código secreto. Los códigos secretos se pueden clasificar en dos categorías primarias: claves de sustitución y claves de transposición.

- **Claves de Sustitución [Visa02]**

  La clave de sustitución reemplaza un carácter del texto en claro con algún otro carácter, que puede ser una letra, un número, o un carácter especial. En la figura 1.2 tenemos un ejemplo, donde se presenta una equivalencia entre los caracteres en claro y los respectivos caracteres equivalentes:

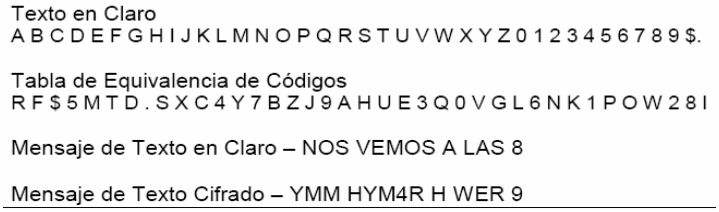


Figura 1.2. Ejemplo de clave de sustitución [Visa02]

- **Claves de Transposición [Visa02]**

  La clave de transposición es una forma más sencilla de la clave de sustitución, en la cual un carácter sustituye a otro siguiendo un patrón predecible. En la figura 1.3 tenemos un ejemplo de la equivalencia establecida entre caracteres en claro y sus caracteres de transposición equivalentes:

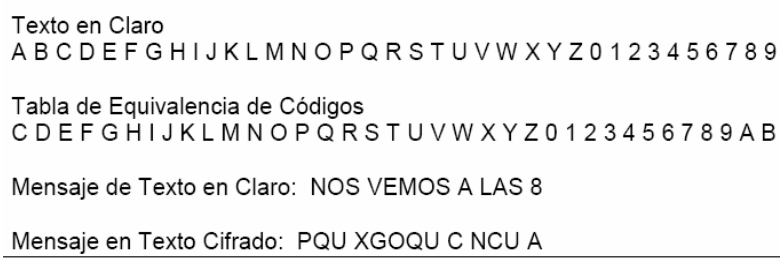


Figura 1.3. Ejemplo de clave de transposición [Visa02]

Para dificultar aún más la labor de descifrar el código, surgió la "clave cifrada en bloque". En una clave cifrada en bloque, el texto cifrado se presenta en grupos de caracteres de una determinada longitud, y se utilizan caracteres de relleno para llenar cualquier grupo incompleto. El principal código utilizado con fines militares por los Estados Unidos durante la Segunda Guerra Mundial era una clave cifrada en bloque cuyos caracteres estaban agrupados en bloques de 5. Utilizando los ejemplos de claves de sustitución y transposición mostrados anteriormente con una longitud de 4 caracteres y caracteres de relleno ABC, obtendríamos el siguiente resultado, que podemos apreciar en la figura 1.4:

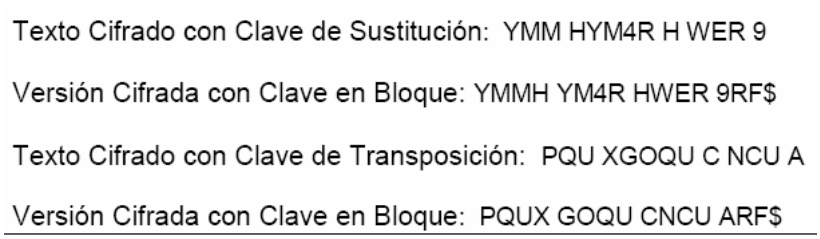


Figura 1.4. Ejemplo de clave en bloque [Visa02]

1.1.3 Tarjetas de Banda Magnética

La tarjeta de banda magnética o tarjeta convencional se desarrolló a finales de los 60 para satisfacer varias necesidades. Una de ellas era permitir a los clientes de los bancos y entidades de ahorro activar y operar de forma rápida y efectiva con los cajeros automáticos. También, para proporcionar un medio con el que operar en puntos de venta específicos.

El objetivo de esta tarjeta era y es identificar a un cliente para acceder a una base de datos remota con la que se establece una conexión. La información que posee la base de datos permite aceptar o rechazar esa transacción.

En la actualidad, la utilización de la tarjeta magnética se ha generalizado de tal forma que, al año, se producen y utilizan una media de 1500 millones de tarjetas magnéticas en el mundo, como podemos ver en la tabla 1.1 basada en información del año 2006:

Estadísticas

Cuatro trimestres finalizados el 30 de septiembre de 2006

	Datos regionales - ALC	Datos mundiales
Tarjetas	249 millones	1.5 mil millones
Transacciones	5.5 mil millones	56.3 mil milliones
Volumen de ventas (US$)	356 mil millones	4.5 billiones
Cajeros automáticos	67.102 mil	1 millón

Tabla 1.1. Estadísticas del uso de tarjetas a nivel mundial [Visa06A]

Adicionalmente, unas 25 000 instituciones financieras proveen las tarjetas y los servicios que permiten a cientos de millones de consumidores y 25 millones de comercios alrededor del mundo beneficiarse de la conveniencia y seguridad del sistema de pagos. [MCWW08]

En 1989, Visa introdujo el programa de Valor de Verificación de Tarjetas (CVV Card Verification Value), como una forma para contrarrestar la epidemia mundial de fraude provocada por la falsificación de la banda magnética. En el

caso de MasterCard, este valor toma el nombre de CVC (Card Verification Code) pero que cumple la misma función que el CVV[1].

El CVV es un código numérico singular que se graba en la banda magnética de la tarjeta. La autorización de transacciones originadas en terminales de lectura de bandas magnéticas incluye la verificación del CVV a los efectos de garantizar que dicho valor coincida con el que tiene el Emisor en el archivo correspondiente a esa cuenta [Visa07].

Hasta la fecha, esta característica ha sido exitosa en la reducción de pérdidas por falsificación, sin embargo, no es infalible. Los delincuentes pueden lograr que la verificación del CVV resulte ineficaz con un nuevo método de falsificación llamado 'skimming', que comenzó varios años atrás con la utilización de terminales de lectura/escritura. La falsificación de banda magnética se ha ido haciendo cada vez más sofisticada, hasta el punto de generar un creciente problema de seguridad de datos utilizando computadoras personales 'laptop' y otros artículos electrónicos. En la actualidad puede sustraerse información de cuentas y duplicarse en prácticamente cualquier punto del proceso de autorización. En el skimming, los delincuentes copian toda la información de una tarjeta válida. Luego graban los datos en tarjetas robadas o falsificadas lo cual da como resultado la aprobación por parte del emisor de transacciones fraudulentas.

1.1.4 Tarjetas Inteligentes

El registro de la primera patente de tarjeta de memoria se produjo en el año 1974 por inventores de Alemania, Japón y Francia. El descenso en el precio de los circuitos integrados y la aparición de las primeras memorias no volátiles,

[1] Para el desarrollo del presente trabajo, se hará referencia a los términos usados por la franquicia Visa Internacional, ya que el Banco de la Nación tiene convenio con esa institución.

indicaban el inicio del desarrollo de esta tecnología, pero debido a la inmadura tecnología de semiconductores, muchos trabajos sobre tarjetas inteligentes estuvieron en investigación y desarrollo hasta la primera mitad de los años ochenta. [Acev+04]

Aparición Cronológica [Medaglia01]

- 1979 Primer prototipo de tarjeta de memoria
- 1982 Primer tarjeta telefónica fabricada para France Telecom
- 1988 Primer tarjeta DES bancaria fabricada para Carte Bancaire
- 1993 Primera tarjeta GSM-SIM (Global System for Mobile Communication)
- 1996 Primer tarjeta RSA 1024 bits "cryptoprocessor"
- 1997 Primer tarjeta de ICC Java powered
- 2000 Primer tarjeta de ICC Windows 2000 powered
- 2000 Primer tarjeta de ICC para SunRay workstation

Desde el comienzo de su desarrollo, las tarjetas inteligentes han demostrado ser un medio ideal para la criptografía. Pueden almacenar de forma segura material criptográfico, claves de cifrado, firmas y certificados digitales, contraseñas e incluso, con el tiempo, patrones biométricos. Por otro lado, destacan por su forma, tamaño y facilidad de manejo, de tal manera que pueden ser empleadas en una variedad de contextos por el usuario. Ésta fue la principal motivación que llevó a las empresas de tecnologías, desarrollar herramientas que permitan trabajar con tarjetas inteligentes.

1.1.5 Fraude en Cajeros Automáticos [Visa06A]

El fraude y compromiso de la información en Cajeros Automáticos han tenido un proceso de introducción acelerado en la Región América Latina y El Caribe a partir del año 1997. Hoy en día el fraude ha ingresado prácticamente a la totalidad de los países.

La intrusión a los equipos incluye una gama de opciones que van desde elementos básicos hasta los tecnológicamente sofisticados, algunos con capacidad de compromiso y almacenamiento de información en volúmenes crecientes, manteniendo como objetivo fundamental el compromiso de información de la banda magnética y el Numero de identificación Personal (PIN por sus siglas en inglés).

El fraude derivado del compromiso de información en ATM representa un gran reto, tanto para los Adquirentes como para los Emisores, ya que existen áreas con oportunidad de mejora en ambos lados del negocio para poderlo controlar y reducir.

Si bien el principio básico para lograr la obtención de la información es la intrusión física al equipo, el fraude en ATM ha estado estrechamente ligado a la inclusión de equipos tecnológicamente más avanzados, así como a la ausencia de mecanismos de monitoreo del cliente en su comportamiento transaccional en los ATM.

Sin embargo no siempre la tecnología ha sido necesaria para que el compromiso sea posible. Implementos físicos y mecanismos básicos han logrado vulnerar los métodos de defensa más tecnificados de los Bancos, por lo que el espectro de compromiso de información y fraude debe ser considerado siempre en toda su gama de posibilidades.

Finalmente la suma de canales y tecnología ha llevado a enaltecer la Seguridad de Información de Cuentas. Ésta como el elemento más importante y valioso tanto para el Banco como para el defraudador. En realidad es la información el principal elemento para que se pueda producir el fraude en cualquier canal o formato.

La bancarización de la población en la Región Latinoamericana continúa siendo uno de los mayores retos de las áreas de Negocio de los Bancos Miembros de Visa Internacional. El cliente, apoyándose en la tecnología (productos, canales de aceptación y comunicación), ha logrado establecer complejas relaciones con las instituciones bancarias, pasando de ser cliente de un producto a cliente multiproductos (crédito, débito, cheques, etc.) así como cliente en un canal de aceptación a cliente multicanales (POS, ATM, banca electrónica, celulares, proximidad y otros).

En particular el uso del ATM se ha convertido en un canal de aceptación masificado que ha permitido a los Bancos reducir costos fijos de operación en agencias y/o sucursales con la ayuda de equipos que permiten la realización de retiro en efectivo, operaciones bancarias y comerciales. El elemento clave para ingresar al ATM en la mayoría de los casos es el uso de un producto de tarjeta de crédito o débito.

Es por ello que la conveniencia de localización y disponibilidad de horario convierten al ATM en un canal prioritario de interacción cliente – Banco, especialmente en segmentos sociales tradicionalmente no bancarizados y que han sido incorporados como los relacionados con nóminas o salarios. Estos elementos que son ampliamente convenientes para el cliente son utilizados por los defraudadores para obtener la información.

Para el Emisor existen varios impactos importantes, no sólo por la pérdida financiera que puede implicar el fraude sino por el cambio de paradigma al momento de reclamación del cliente y la confianza de éste en el uso del medio de pago.

Tradicionalmente la reclamación del cliente estaba cubierta por la digitación del PIN como equivalente a su presencia al momento de la transacción. Sin embargo dada la magnitud de los reclamos y la presencia de entidades gubernamentales

de protección al consumidor, aunado al reconocimiento y existencia del problema de fraude en ATM, los Bancos Emisores han tenido que replantear la forma de recepción y tramitación de las reclamaciones. Este proceso conlleva costos de operación, administración e investigación adicionales.

De igual manera la confianza del cliente hacia el Banco, el medio de pago y el canal, en este caso el ATM, se ve seriamente afectada. Ante esta situación el Emisor se ve obligado a realizar un proceso más proactivo de detección de compromiso de información y prevención de fraude.

1.1.6 Franquicias

Las franquicias, concesiones o licencias, son acuerdos contractuales mediante los cuales una compañía matriz (franquiciadora) le concede a una pequeña compañía a un individuo (franquiciador) el derecho de hacer negocios en condiciones específicas. Lo dicho anteriormente, nos permite resumir de forma simple, que un franquiciador tiene el derecho de nombre o de marca registrada y le vende el derecho a un franquiciado; conociendo esto como licencia de producto [D'Andrea98]

El origen del contrato de franquicia se remonta a unos 150 años atrás. Un ejemplo temprano lo constituye la característica apariencia de los hoteles históricos en Nueva Gales del Sur para los que se realizaban contratos de franquicia entre los cerveceros y los hoteleros. Un ejemplo americano lo constituyó el sistema de telégrafo eléctrico que gestionaban varias compañías de ferrocarriles pero que estaba controlado por la Western Union.

La franquicia moderna tuvo su espaldarazo en la década de 1950 con el auge de los restaurantes de comida rápida entre los cuales McDonald's fue el primero en cosechar un éxito global. Muchos sectores detallistas están ahora dominados por

el sistema de franquicia hasta el punto de que los establecimientos gestionados individualmente son la excepción más que la regla. [Wikipedia08b]

1.1.7 Tarjetas Multired Global Débito

El 31 de mayo del 2007 se dio el lanzamiento de la alianza estratégica entre Visa Internacional y el Banco de la Nación, a través de la implementación de las tarjetas Multired Global Débito. Gracias a este acuerdo, la amplia red de cajeros automáticos del Banco de la Nación puede ser utilizada por los clientes nacionales y extranjeros de cualquier banco comercial o institución financiera afiliada a la red Visa Internacional, para realizar sus retiros en efectivo. De la misma manera, a través del uso de las tarjetas Multired Global Débito, los clientes del Banco de la Nación que cuenten con este servicio, podrán hacer uso de los cajeros automáticos de otras entidades bancarias afiliadas a Visa.

Actualmente existen cinco millones de peruanos con algún tipo de tarjeta Visa de los diversos bancos nacionales y extranjeros con sede en el Perú, y muchos de los miles de turistas que llegan a nuestro país diariamente lo hacen con tarjetas afiliadas a la red de Visa Internacional, quienes ahora podrán hacer uso de sus cajeros automáticos. Todos ellos se sumarán al 1’668,152 de clientes Visa que ya existen en el Banco de la Nación.

El Banco de la Nación cuenta con aproximadamente 520 cajeros automáticos en todo el país, algunos de los cuales están ubicados en lugares donde no existe otra oferta bancaria. Es preciso mencionar que la red de cajeros del Banco de la Nación representa el 24 por ciento de la totalidad de cajeros automáticos del sistema bancario, lo que hace sumamente importante el acuerdo logrado con Visa. [BNCC07]

1.2 Definición del Problema

Con el creciente número de clientes y como consecuencia de la globalización, muchos bancos deciden lanzar nuevos productos de crédito y débito con la marca de franquicias internacionales, que permitan que dichos productos puedan ser utilizados a nivel internacional y paralelamente, permitir que clientes de otros bancos puedan hacer uso de sus cajeros automáticos y demás servicios.

El problema se genera ya que debido al número exponencialmente creciente de fraudes, suplantación de identidad, 'skimming' y otros, causados por el avance y disponibilidad de la tecnología a personas indeseables, la arquitectura actual de seguridad de información de la mayoría de los bancos no garantiza a sus clientes, ni a los nuevos usuarios de otros bancos, un nivel adecuado de confidencialidad, integridad y disponibilidad de los datos expuestos en la red.

El Banco de la Nación ha implementado el algoritmo criptográfico DES para la seguridad de las transacciones en cajeros automáticos y la protección de información de clientes, utilizando la marca de Visa Internacional, siendo el algoritmo DES vulnerable a ser corrompido.

Como último punto, Visa Internacional solicita la implementación de un algoritmo más seguro para el año 2010 a todas aquellas instituciones que utilicen su marca, por lo que el Banco de la Nación requiere en el mediano plazo cambiar no sólo de algoritmo, sino de implementar controles de administración de las claves criptográficas que se utilicen para encriptar dicha información, de manera que aprueben el "Programa de Auditoría del PIN" de Visa Internacional, y puedan certificarse con el Rol Emisor y Adquirente, considerando que los cambios deberá enfocarse en el canal de cajeros automáticos.

1.3 Objetivos

1.3.1 General

Definir controles de seguridad de información para el proceso de administración de las claves criptográficas usadas para encriptar la información de los cajeros

automáticos del Banco de la Nación, considerando el cambio de la estructura de encripción, de DES a EMV.

1.3.2 Específicos

- Identificar los riesgos en las transacciones con tarjetas de banda magnética Multired Global Débito del Banco de la Nación en el canal de cajeros automáticos, así como en la administración de las claves que actualmente se usan para la encripción y desencripción de información.
- Definir los cambios necesarios para la migración de DES a EMV, utilizando la infraestructura tecnológica existente.
- Cumplir con las especificaciones de seguridad del PIN de Visa Internacional para obtención de la certificación de Rol Emisor y Rol Adquirente.

1.4 Justificación

La migración de algoritmo DES a EMV es posible para el Banco de la Nación, sin realizar un gasto económico significativo, ya que su infraestructura actual soporta el cambio de algoritmo (infraestructura basada en equipos de seguridad HSM 8000).

La justificación teórica del uso del estándar EMV es que este estándar es reconocido a nivel mundial para las tres marcas más importantes de franquicias de tarjetas de débito y crédito, incorporando los niveles de seguridad de información brindados por el uso de tecnología chip, en lugar de la banda magnética, la cual está siendo clonada fácilmente en todos los países del mundo.

La justificación práctica está orientada básicamente para el Banco de la Nación, el cual podría lograr una implementación de controles basados en el estándar EMV utilizando las tecnologías existentes en su plataforma. Para ello se presentarán los criterios básicos bajo los cuales las claves criptográficas involucradas en el proceso de encripción y desencripción de información de los cajeros automáticos del Banco de la Nación, deberán ser presentadas, inscritas, almacenadas, generadas, transportadas, modificadas y

eliminadas de manera segura; a comparación del algoritmo DES utilizado actualmente, el cual como se ha demostrado de manera matemática por muchos científicos, puede ser corrompido muy rápidamente.

A pesar que existen controles determinados de manera general, este trabajo buscará determinar los controles de manera personalizada para el Banco de la Nación, no sólo a nivel tecnológico sino principalmente a nivel administrativo.

Adicionalmente, los controles pueden ser adaptados fácilmente para cualquier otra entidad financiera, ya que hasta la fecha ningún banco ha implementado de manera integral, el uso de tarjetas inteligentes.

Aquí se presenta un cuadro comparativo básico entre el algoritmo DES y EMV a nivel de seguridad de información, que nos ayudará a definir las principales diferencias entre ambos, y que posteriormente serán detallados en el Marco Teórico y en el Estado del Arte:

Algoritmo DES	Estándar EMV
Algoritmo simétrico, es decir, el emisor como el receptor comparten una misma llave criptográfica.	Algoritmo Asimétrico, es decir, el emisor y el receptor tienen llaves criptográficas diferentes que se corresponden matemáticamente.
Cada llave criptográfica tiene una longitud de de 56 bits, lo cual lo hace más vulnerable	Cada llave criptográfica tiene una longitud de 128 bits
Deben ser encriptadas bajo otras llaves y enviados sus componentes bajo el riesgo de ser interceptados.	Son soportadas por Infraestructura de Llave Pública, lo cual les permite ser transportadas por la red de manera segura.
Utilizados en el mundo de las tarjetas de débito y crédito a través de la banda magnética.	Pueden ser usadas en tarjetas de débito y crédito a través de tecnología chip.
No garantizan el No Repudio	Garantizan el No Repudio

Tabla 1.2. Comparación de DES y EMV

1.5 Propuesta

Para alcanzar a desarrollar la propuesta de solución, se ha realizado una investigación a profundidad sobre la infraestructura tecnológica del Banco de la Nación, así como la infraestructura criptográfica que se implementó para el uso de tarjetas Multired Global

Débito bajo la marca de Visa Internacional. Esto servirá de base para determinar los parámetros relevantes para migrar las claves criptográficas DES a EMV.

Así mismo se investigó sobre los parámetros de seguridad de información considerados por franquicias internacionales como Visa, MasterCard y Europay para autorizar a las entidades bancarias el uso de sus marcas tanto como Rol Emisor como Rol Adquirente.

Con esta información se desarrollarán los controles para la administración de las claves criptográficas EMV que se utilizarían en las transacciones de cajeros automáticos del Banco de la Nación. Esto consiste en la generación, presentación, inscripción, almacenamiento, transporte, reemplazo y eliminación de dichas claves criptográficas. Estos controles estarán alineados a los parámetros básicos de cumplimiento, establecidos por Visa Internacional para las entidades emisoras y adquirentes de su marca. Se considerarán también controles establecidos por otras franquicias y especialistas en seguridad de información, así como las mejores prácticas establecidas por organizaciones de estandarización, tales como ISO, NIST, FIPS y otras.

1.6 Organización de la Tesina

Para presentar el presente trabajo de manera entendible, se ha dividido en capítulos. En el capítulo 2 se presenta el Marco Teórico, dividido en Definiciones Teóricas y Marco Conceptual. En el capítulo 3 se presenta el Estado del Arte de la Estructura de Llaves Criptográficas, Equipos de Seguridad, Organización del Banco de la Nación, así como el estándar EMV. En el capítulo 4 se realiza la evaluación de riesgos del estado actual de la criptografía del banco, para presentar los controles de seguridad de información asociados a las llaves criptográficas de los cajeros automáticos en el capítulo 5. En el capítulo 6 se encuentran las conclusiones y trabajos futuros; en el capítulo 7, el glosario de términos y finalmente, en el capítulo 8, las referencias bibliográficas. Las referencias bibliográficas citadas a lo largo del documento, se escribirán entre corchetes "[ ]" y se detallarán, como se ha mencionado, en el capítulo 8, notas al pie de por lo cual no se usarán notas al pie de página.

Capítulo 2: Marco Teórico

En este capítulo se describirán los conceptos fundamentales relacionados a la infraestructura actual del Banco de la Nación y a la solución propuesta.

2.1 Definiciones Teóricas

2.1.1 Confidencialidad

Es la propiedad de la seguridad de información que permite mantener en secreto la información y sólo los usuarios autorizados pueden manipularla. Los usuarios pueden ser personas, procesos, programas, u otros. [Acev+04]

Protege a los activos de información contra accesos o divulgación no autorizados. [INEI02]

2.1.2 Integridad

La integridad de la información corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero. Garantiza la exactitud de los activos de información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta. [INEI02]

La integridad abarca los siguientes aspectos:

- Que no se realicen modificaciones por personas no autorizadas a los datos, información o procesos
- Que no se realicen modificaciones no autorizadas por personal autorizado a los datos, información o procesos
- Que los datos o información sea consistente tanto interna como externamente. [Wikipedia08a]

Mantener la integridad es importante para verificar que en el tiempo de viaje por la Red de la información entre el sitio emisor y receptor nadie no autorizado pueda modificar el mensaje. [Acev+04]

2.1.3 Disponibilidad

Asegura que los recursos informáticos y los activos de información pueden ser utilizados en la forma y tiempo requeridos. Bajo el punto de vista de seguridad, la disponibilidad se refiere a su posible recuperación en caso de desastre (recuperabilidad), y no al concepto de nivel de servicio empleado en otras áreas. [INEI02]

2.1.4 Autentificación

La autentificación es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información. Por entidad se entiende tanto personas, como procesos o tecnologías.

Existen varias formas de poder autentificarse:

- Basada en claves
- Basada en direcciones
- Criptográfica
- Biometría (huellas digitales, retina del ojo, la voz u otros)

La autentificación puede realizarse a través de tres características: algo que somos, algo que tenemos, algo que sabemos. A partir de esto se crean dos tipos de autentificación: *autentificación débil,* cuando utiliza sólo una característica de las mencionadas anteriormente; y *autentificación fuerte,* cuando se utiliza al menos dos de las tres características mencionadas.

2.1.5 No-Repudio

Los servicios de no-repudio ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida.

Se aplica en ambos lados de la comunicación, tanto para no poder rechazar la autoría de un mensaje, como para negar su recepción. [Acev+04]

2.1.6 Continuidad del servicio [Jones08B]

La administración de seguridad no se detiene con la prevención. Las cosas pueden salir mal, independientemente de qué tan bien se controlen las amenazas y las vulnerabilidades, y se implementen los controles de acceso. Una administración de seguridad prudente refleja que la empresa asume la posibilidad de que alguna vez existan fallas dentro de su infraestructura de TI. Las fallas no se limitan a las violaciones de la seguridad, aunque, los desastres naturales, las fallas eléctricas, el funcionamiento defectuoso del hardware y las fallas del software pueden afectar la habilidad de la organización para funcionar. La continuidad del servicio es la práctica o preparación para dichas complicaciones y la creación de estrategias para recuperar con el mínimo impacto posible las operaciones de la empresa. Los principales aspectos de las prácticas para la continuidad del servicio son:

- Identificar los requisitos de la empresa para la continuidad del servicio
- Formular planes de respaldo y recuperación
- Explorar las mejores prácticas para mantener la continuidad del servicio

Como sucede con otras áreas de la administración de seguridad, la continuidad de los servicios y otras operaciones de TI se superponen en gran medida. En el caso de la continuidad del servicio, gran parte pertenece al área de administración de almacenamiento. Por supuesto, la administración de almacenamiento no trata sólo de la continuidad del servicio, así como la administración de seguridad abarca más que la continuidad del servicio. Las dos, sin embargo, están estrechamente combinadas, y las técnicas desarrolladas en ambas áreas se complementan entre sí para proporcionar un enfoque integral destinado a la planificación de la continuidad del servicio.

El primer paso para comprender el alcance de los requisitos de la continuidad del servicio es comprender los datos y activos necesarios para mantener las operaciones de la organización. La planificación de la continuidad del servicio no consiste simplemente en el respaldo de todos los datos, en el almacenamiento de medios de respaldo fuera del sitio o en la restauración de los datos según sea necesario. Aunque ese enfoque puede funcionar para empresas muy pequeñas, la mayoría de las organizaciones con infraestructuras de TI han evolucionado hacia entornos más complejos que requieren una amplia gama de soluciones.

El nivel básico de la funcionalidad incluye aquellos servicios necesarios para asegurar las operaciones esenciales (los sistemas operativos y los hardware básicos también se incluyen dentro del punto de recuperación), así como también aquellos que se encuentran adjuntos a los flujos de ingresos o que requieren por norma. Si estos sistemas no funcionan, la empresa no puede llevar a cabo sus operaciones de negocio.

2.1.7 Evaluación de Riesgos

La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un número de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales. [INDECOPI07]

2.1.8 Conceptos de Sistemas de Pagos

En un sistema de pago interactúan las siguientes entidades:

- **Tarjetahabientes:** aquella persona que tiene una tarjeta a través de un contrato con un emisor. Debe elegir, recordar y actualizar su PIN, así como presentar su tarjeta en un equipo de pago, como un ATM.
- **Emisor:** es una entidad que emite Tarjetas, y cuyo nombre aparece en la tarjeta como el Emisor. Los Emisores identifican a su público y distribuyen tarjetas de Crédito o Débito que le permite realizar transacciones al Tarjetahabiente sin necesidad de efectivo. Cada Emisor determina sus tasas, servicios, límites, y otros parámetros esenciales.
- **Adquirente:** es una entidad miembro que adquiere las transacciones de un Comercio o desembolsa dinero a un Tarjetahabiente a través de un Cajero Automático u Oficina. Es el Miembro que directa o indirectamente presenta al Emisor la Transacción para cobro a través del Sistema al cual se encuentre conectado. La mayoría de los Adquirentes contratan con comercios para procesar sus transacciones, o proveen servicio de efectivo; por ejemplo, Cajeros Automáticos.

En la figura 2.1 podemos apreciar la interacción entre las entidades emisoras y adquirentes. En este caso el 'Switch' es el punto de conexión de Visanet Perú o Visa Internacional (para transacciones domésticas o internacionales respectivamente), al cual se conectan todas las entidades que trabajan con su marca. Cabe resaltar que una entidad puede contar con permiso de Visa Internacional, bajo ciertos controles, para trabajar bajo los roles de emisor y adquirente de manera simultánea.

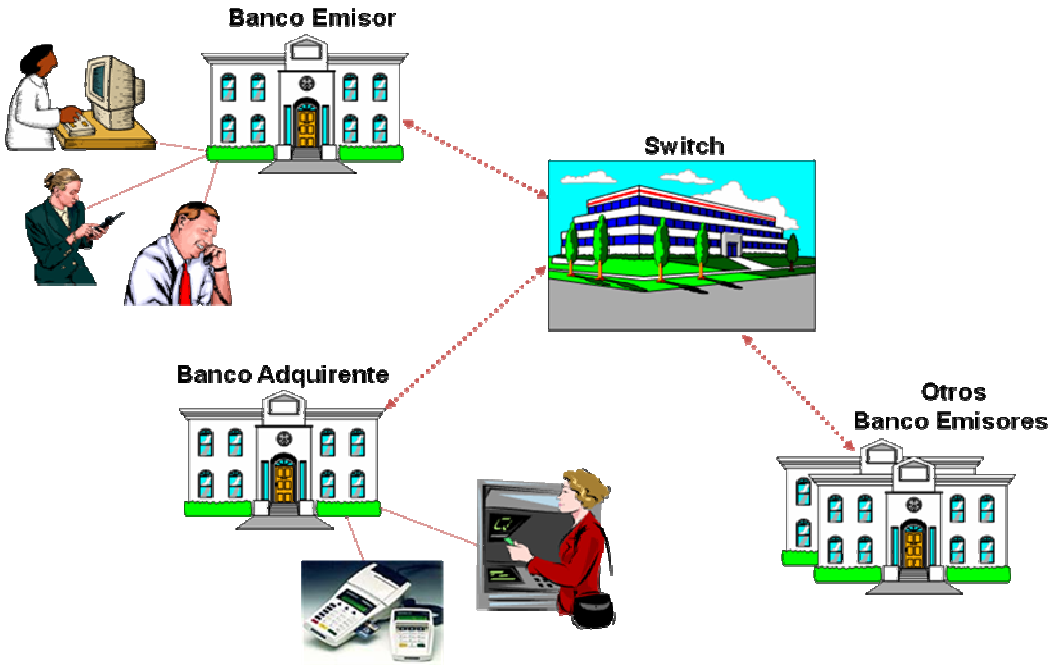


Figura 2.1. Esquema de interconexión de entidades [Thales05]

- **BID Business Identification:** Identificador del negocio - el número único de 8 dígitos asignado por Visa a cada Miembro de la Asociación. Una vez que una Institución es aprobada como un Miembro Visa, el Departamento Legal asigna un número de identificación del negocio.

- **Transacción On-Us:** El Emisor de la Tarjeta y el Adquirente/Comercio o ATM es la misma entidad.

- **Transacción Doméstica:** El Emisor de la Tarjeta y el Adquirente/Comercio se encuentran en el mismo país.

- **Transacción Internacional:** El Emisor de la Tarjeta y el Adquirente/Comercio se encuentran en diferentes países.

2.1.9 Llaves Criptográficas [Lucena99]

Según el Diccionario de la Real Academia, la palabra Criptografía proviene del griego *Krytoc*, que significa oculto, y *Grafos*, que significa escritura, y su definición es: *"Arte de escribir con clave secreta o de un modo enigmático"*. Obviamente la Criptografía hace años que dejó de ser un arte para convertirse en una técnica, o más bien un conglomerado de técnicas, que tratan sobre la protección –ocultamiento frente a observadores no autorizados- de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Teoría de Números (o Matemática Discreta), que estudia las propiedades de los números enteros, y la Complejidad Algorítmica.

El cifrado es el proceso por el cual cierta información se transforma en información cifrada a través de un algoritmo y una llave. El descifrado a su vez es el proceso por el cual recuperamos la información original al aplicar un algoritmo y una llave a la información cifrada. Así los elementos básicos de la criptografía son los algoritmos de cifrado y descifrado así como la llave. La llave determina el tipo de transformación que se realiza sobre los datos y elementos de información. En los sistemas computacionales e informáticos, la llave es una cadena de datos (almacenada electrónicamente).

Existen dos documentos fundamentales, uno escrito por Claude Shannon en 1948 ("A Mathematical Theory of Communication"), en el que se sientan las bases de la Teoría de la Información, y que junto con otro artículo posterior del mismo autor sirvió de base para la Criptografía moderna. El segundo trabajo fundamental, publicado por Whitfield Diffie y Martin Hellman en 1976, se titulaba "New directions in Cryptography", e introducía el concepto de Criptografía de Llave Pública, abriendo enormemente el abanico de aplicación de esta disciplina.

Conviene hacer notar que la palabra Criptografía sólo se refiere al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos (Criptoanálisis). El término Criptología, aunque no está recogido aún en el Diccionario, se emplea habitualmente para agrupar estas dos disciplinas.

Criptosistema

Definiremos un criptosistema como una quíntupla (M, C, K, E, D), donde:

- M representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano o texto claro) que pueden ser enviados.
- C representa el conjunto de todos los posibles mensajes cifrados, encriptados o criptogramas.
- K representa el conjunto de claves que se pueden emplear en el criptosistema.
- E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_k para cada valor posible de la clave k.
- D es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k (E_k (m)) = m$$

Es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

Existen dos tipos fundamentales de criptosistemas:

a. Criptosistemas simétricos o de llave privada. Son aquellos que emplean la misma clave k tanto para cifrar como para descifrar. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la llave a usar. Una vez ambas tienen acceso a esta llave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma llave. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitir la clave de forma segura. El mecanismo de cifrado y descifrado de información encriptada bajo un algoritmo simétrico se presenta en la figura 2.2:

Figura 2.2. Modelo de encriptación/desencriptación con claves simétricas [Visa06B]

b. Criptosistemas asimétricos o de llave pública, que emplean una doble clave (k_p; k_P). k_p se conoce como clave privada y k_P se conoce como clave pública. Una de ellas sirve para la transformación E de cifrado y la otra para la transformación de de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública k_P no permita calcular la clave privada k_p. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros (puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar), o para llevar a cabo autenticaciones. En la figura 2.3 se puede apreciar el mecanismos de cifrado de información bajo algoritmos asimétricos:

Figura 2.3. Modelo de encriptación/desencriptación con claves asimétricas [Visa06B]

Secuencias Aleatorias

Los algoritmos de llave pública, debido a su mayor orden de complejidad, suelen ser empleados en conjunción con algoritmos de llave privada de la siguiente forma: el mensaje primero se codifica empleando un algoritmo simétrico y la llamada clave de sesión, que sería diferente cada vez. Es la clave de sesión la que se codifica empleando criptografía asimétrica. La única manera de que estas claves sean seguras es que no exista ningún tipo de dependencia entre una clave y la siguiente, esto es, que sean aleatorias. De aquí surge el interés por los números aleatorios en Criptografía.

a. Secuencias pseudoaleatorias

   En realidad es casi del todo imposible generar secuencias auténticamente aleatorias en una computadora, puesto que estas máquinas son, en teoría, completamente deterministas. Todos los generadores pseudoaleatorios producen secuencias finitas y periódicas de números empleando operaciones aritméticas y/o lógicas. Lo único que podremos conseguir es que estas secuencias sean lo más largas posible antes de comenzar a repetirse y que superen los tests estadísticos de aleatoriedad.

   Dentro de este tipo de secuencias, tenemos las Secuencias estadísticamente aleatorias, las cuales superan los tests estadísticos de aleatoriedad.

b. Secuencias criptográficamente aleatorias

Para que una secuencia pseudoaleatoria sea criptográficamente aleatoria, ha de cumplir la propiedad de ser impredecible. Esto quiere decir que debe ser computacionalmente intratable el problema de averiguar el siguiente número de la secuencia, teniendo total conocimiento acerca de todos los números anteriores y del algoritmo de generación empleado.

c. Secuencias totalmente aleatorias

Como ya se ha dicho antes, no existe la aleatoriedad cuando se habla de computadoras. En realidad se puede decir que no existen en el Universo sucesos cien por cien aleatorios. En cualquier caso, y a efectos prácticos, consideraremos un tercer tipo de secuencias pseudoaleatorias: secuencias aleatorias, una secuencia es totalmente aleatoria (o simplemente aleatoria) si no puede ser reproducida de manera fiable.

Texto Plano

Es el conjunto de números y caracteres que se necesita encriptar. También recibe el nombre de texto en claro.

Texto Cifrado

Es el texto resultante de la encripción del texto plano bajo una llave de encripción.

2.1.10 El Algoritmo DES [Lucena99]

Data Encryption Standard (DES), normado por el estándar FIPS 46-1 en 1977. También definido como ANSI Standard X3.92. El NIST recertificó el DES en 1993. Este algoritmo utiliza la función de sustitución: S-Caja o caja de sustitución.

Una S-Caja de m*n bits es una tabla de sustitución que toma como entrada cadenas de m bits y da como salida cadenas de n bits. DES, por ejemplo, emplea ocho S-Cajas de 6*4 bits. La utilización de las S-Cajas es sencilla (ver figura 2.4): se divide el bloque original (R_i) en trozos de m bits y cada uno de ellos se sustituye por otro de n bits, haciendo uso de la S-Caja correspondiente. Normalmente, cuanto más grandes sean las S-Cajas, más resistente será el algoritmo resultante, aunque la elección de los valores de salida para que den lugar a un buen algoritmo no es en absoluto trivial.

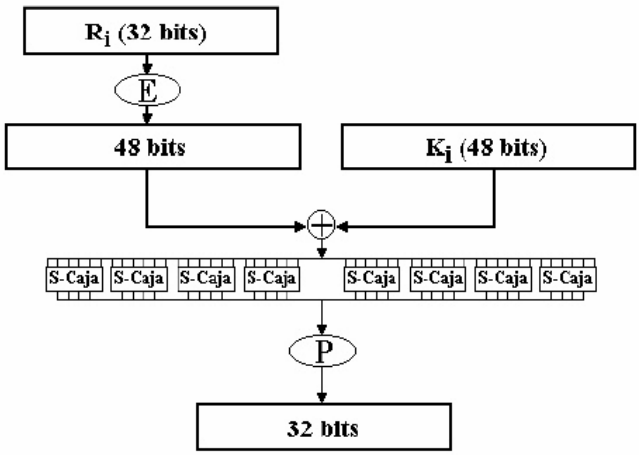


Figura 2.4. Esquema de la función f del algoritmo DES [Lucena99]

El algoritmo DES es el algoritmo simétrico más extendido mundialmente. Data de mediados de los setenta, cuando fue adoptado como estándar para las comunicaciones seguras por el Gobierno de los EE.UU. En realidad la NSA lo diseño para ser implementado por hardware, con la intención de mantenerlo en secreto, pero al parecer por un malentendido entre ellos y la Oficina Nacional de Estandarización, su especificación se hizo pública con suficiente detalle como para que cualquiera pudiera implementarlo por software. No fue casualidad que el siguiente algoritmo adoptado (Skipjack) fuera mantenido en secreto.

A mediados de 1998, se demostró que un ataque por la fuerza bruta a DES era viable, debido a la escasa longitud que emplea en su clave. No obstante, el

algoritmo aún no ha demostrado ninguna debilidad grave desde el punto de vista teórico, por lo que su estudio sigue siendo plenamente interesante.

El algoritmo DES codifica bloques de 64 bits empleando claves de 56 bits. Es una Red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio (P_i) y otra que se aplica al final (P_f), tales que $P_i = P_f^{-1}$.

La función f (figura 2.4) se compone de una permutación de expansión (E), que convierte el bloque de 32 bits correspondiente en uno de 48. Después realiza un or-exclusivo (XOR según tabla 2.1) con el valor K_i, también de 48 bits, aplica ocho S-Cajas de 6*4 bits, y efectúa una nueva permutación P.

P	Q	Salida
0	0	0
0	1	1
1	0	1
1	1	0

Tabla 2.1. Operación lógica XOR

Se calcula un total de 16 valores de K_i (figura 2.5), uno para cada ronda, efectuando primero una permutación inicial EP_1 sobre la clave de 64 bits, llevando a cabo desplazamientos a la izquierda de cada una de las dos mitades -de 28 bits- resultantes, y realizando finalmente una elección permutada (EP_2) de 48 bits en cada ronda, que será la K_i. Los desplazamientos a la izquierda son de dos bits, salvo para las rondas 1, 2, 9 y 16, en las que se desplaza sólo un bit. Nótese que aunque la clave para el algoritmo DES tiene en principio 64 bits, se ignoran ocho de ellos -un bit de paridad por cada byte de la clave-, por lo que en la práctica se usan sólo 56 bits.

Para descifrar basta con usar el mismo algoritmo (ya que $P_i = P_f^{-1}$) empleando las K_i en orden inverso.

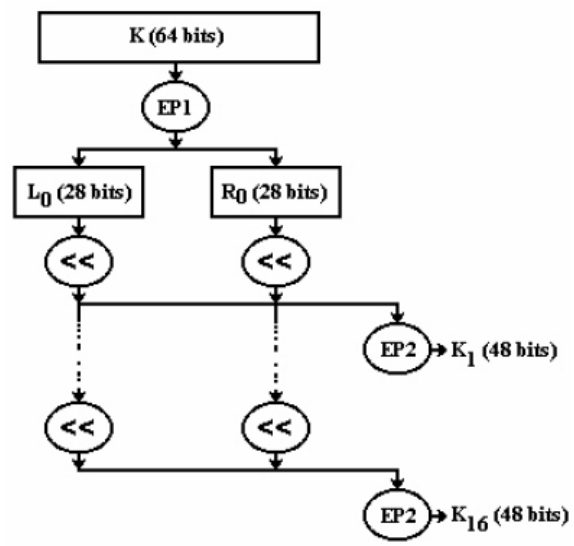


Figura 2.5. Cálculo de las K_i para el algoritmo DES [Lucena99]

A mediados de julio de 1998, una empresa sin ánimo de lucro, llamada EFF (Electronic Frontier Foundation), logró fabricar una máquina capaz de descifrar un mensaje DES en menos de tres días. Curiosamente, pocas semanas antes, un alto cargo de la NSA había declarado que dicho algoritmo seguía siendo seguro, y que descifrar un mensaje resultaba aún excesivamente costoso, incluso para organizaciones gubernamentales. DES-Cracker costó menos de 40 millones de pesetas.

A pesar de su caída, DES sigue siendo ampliamente utilizado en multitud de aplicaciones, como por ejemplo las transacciones de los cajeros automáticos. De todas formas, el problema real de DES no radica en su diseño, sino en que emplea una clave demasiado corta (56 bits), lo cual hace que con el avance actual de las computadoras los ataques por la fuerza bruta comiencen a ser opciones realistas. Mucha gente se resiste a abandonar este algoritmo, precisamente porque ha sido capaz de sobrevivir durante veinte años sin mostrar ninguna debilidad en su diseño, y prefieren proponer variantes que, de un lado evitarían el riesgo de tener que confiar en algoritmos nuevos, y de otro permitirían aprovechar gran parte de las implementaciones por hardware existentes de DES.

2.1.11 Algoritmos asimétricos [Lucena99]

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos se recomiendan claves de al menos 1024 bits. Además, la complejidad de cálculo que comportan estos últimos los hace considerablemente más lentos que los algoritmos de cifrado por bloques. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje.

Los algoritmos asimétricos poseen dos claves diferentes en lugar de una, K_p y K_P, denominadas clave privada y clave pública. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra.

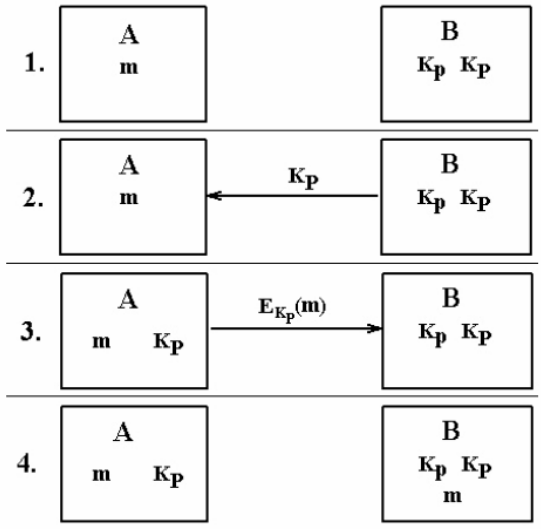


Figura 2.6. Transmisión de información empleando algoritmos asimétricos [Lucena99]

Como podemos ver en la figura 2.6, en (1) A tiene el mensaje m y quiere enviárselo a B; (2) B envía a A su clave pública, K_P; (3) A codifica el mensaje m y envía a B el criptograma EK_P (m); (4) B decodifica el criptograma empleando la clave privada K_p.

Autentificación

Otra aplicación de los algoritmos asimétricos es la autentificación de mensajes, con ayuda de funciones resumen, que nos permiten obtener una firma a partir de un mensaje. Dicha firma es mucho más pequeña que el mensaje original, y es muy difícil encontrar otro mensaje que tenga la misma firma. Supongamos que A recibe un mensaje m de B y quiere comprobar su autenticidad. Para ello B genera un resumen del mensaje r(m) y lo codifica empleando la clave de cifrado, que en este caso será privada. La clave de descifrado se habrá hecho pública previamente, y debe estar en poder de A. B envía entonces a A el criptograma correspondiente a r(m). A puede ahora generar su propia r'(m) y compararla con el valor r(m) obtenido del criptograma enviado por B. Si coinciden, el mensaje será autentico, puesto que el único que posee la clave para codificar es precisamente B.

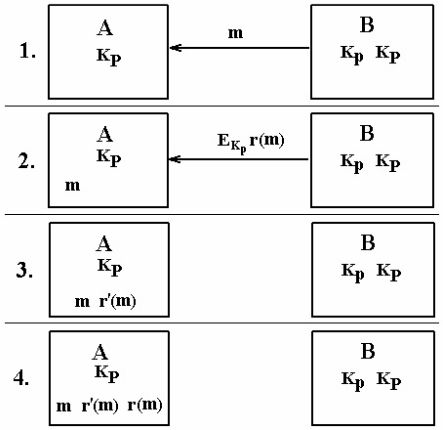


Figura 2.7. Autentificación de información empleando algoritmos asimétricos [Lucena99]

Según muestra la figura 2.7; (1) A, que posee la clave pública K_P de B, recibe el mensaje m y quiere autentificarlo; (2) B genera el resumen de m envía a A el criptograma asociado $EK_p(r(m))$; (3) A genera por su cuenta r'(m) y decodifica el criptograma recibido usando la clave K_P; (4) A compara r(m) y r'(m) para comprobar la autenticidad del mensaje m.

2.1.12 Public Key Infrastructure (PKI) [Ponce04]

a. Firma digital

- La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que estos gocen de una característica que únicamente era propia de los documentos en papel.
- Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.
- Detecta cambios al contenido de la transacción durante la transmisión.
- Para firmar un documento digital, su autor utiliza su propia clave secreta a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no repudio).
- La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.
- En el Perú, las respaldan las siguientes leyes
  - Ley No. 27269 "Ley de Firmas y Certificados Digitales", del 08-Mayo-2000, con el objetivo de regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.
  - Ley No. 27291 "Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica", del 23-Junio-2000.
- La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan al documento firmado con información propia del firmante (persona que firma electrónicamente el documento),

y permiten que terceras partes puedan reconocer la identidad de la persona y asegurarse que los contenidos no han sido modificados.

- El firmante genera, mediante una función matemática, una huella digital del mensaje. Esta huella digital se cifra con la clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.
- Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifra la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.
- Para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por una *Autoridad Certificante.*

b. Certificados digitales

- Son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado.
- Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.
- Objetivos:
  - Autenticación: verificación de la identidad de las partes de una transacción.
  - Integridad: garantiza que los datos no sean alterados.
  - No repudio: Previene la desaprobación de una transacción.

- Confidencialidad: Protege a la información sensible de ser vista indiscriminadamente.
- Control de Acceso: Provee evidencias duraderas y confiables de la transacción después que ésta ocurre.

- Los certificados contienen:
  - El nombre del titular de la firma digital o sello digital, que deberá estar identificado de forma inequívoca.
  - La clave pública atribuida al mismo.
  - El nombre de los algoritmos utilizados para la emisión del Certificado Digital.
  - El número de Serie del certificado.
  - La fecha de inicio y final de la validez del certificado.
  - El nombre de la entidad certificadora y su firma digital.
  - Información sobre las limitaciones que se hayan establecido para su utilización e información relativa a certificados asociados.
- Habitualmente, un certificado también contiene una fecha de expiración, el nombre de la Autoridad Certificante que emitió ese certificado, un número de serie y alguna otra información.
- Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del certificado.
- El Certificado es una representación digital de la tarjeta física
- El Certificado representa la marca del Miembro
- El formato de los certificados está definido por el estándar internacional ITU-T X.509. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.
- X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, define una estructura estándar para los certificados de clave pública y un método para generar las listas de certificados revocados. Dicha estructura sirve

de base para los estándares PKIX desarrollados por el PKIX Working Group del Internet Engineering Task Force.

c. Autoridad Certificadora

- Emite certificados a entidades y a otras Autoridades Certificadoras según el flujo de la figura 2.8.
- Autentica a quienes solicitan los certificados antes de emitirlos
- Establece políticas que gobiernan el uso de los Certificados que emite
- Valida los Certificados para su uso
- Contiene la Lista de Revocación de Certificados (CRL), es decir aquellos certificados que han perdido su validez.

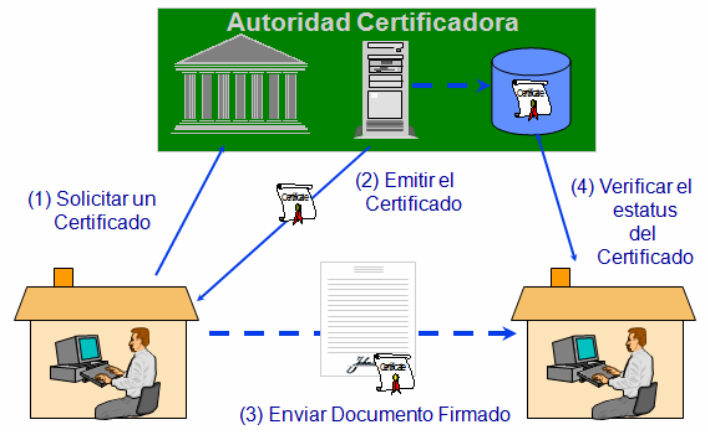


Figura 2.8. Generación de Certificados digitales [Visa06B]

d. Proceso de Firma

- El emisor encripta el documento con su llave privada, enviando al destinatario tanto el documento en claro como el encriptado.
- El receptor desencripta el documento cifrado con la clave pública del emisor y comprueba que coincide con el documento original, lo que atestigua de forma total la identidad del emisor.

- El método de la firma digital no sólo proporciona autenticidad del mensaje enviado por el emisor, sino que también asegura el no repudio, ya que sólo el dueño de una llave privada puede encriptar un documento de tal forma que se pueda desencriptar con su llave pública.
- Asimismo proporciona Integridad de datos, ya que si el documento fuera accedido y modificado en el camino el resumen del documento cambiaría también.

2.1.13 Banda Magnética

La composición de la Banda Magnética actual, implementada bajo el algoritmo DES está normada por las siguientes reglas internacionales:

- Data Encryption Algorithm ANSI X3.92-1981.
- Personal Identification Number (PIN) Management and Security ANSI X9.8-1982.
- Personal Identification Number Management and Security ISO 9564-1991.
- Modes of Data Encryption Algorithm Operation ANSI X.106-1983.
- Financial Institution Key Management (Wholesale) ANSI X9.17-1985.
- Financial Institution Retail Message Authentication ANSI X9.19-1986.
- Financial Services Retail Key Management ANSI X9.24-1992.

Las pistas de la banda magnética se componen de la siguiente manera:

- Pista 1: que contiene un máximo de 79 caracteres distribuidos según nos muestra la siguiente figura:

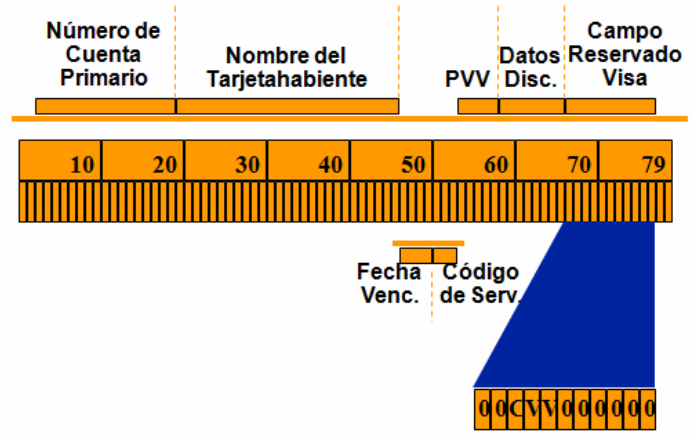


Figura 2.9. Composición de la Pista 1 [Visa06B]

- Pista 2: que contiene un máximo de 40 caracteres distribuidos según nos muestra la figura:

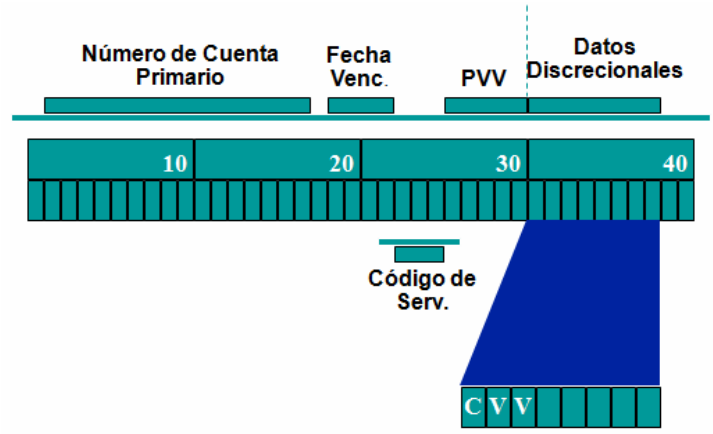


Figura 2.10. Composición de la Pista 2 [Visa06B]

2.1.14 Tarjetas Inteligentes [Medaglia01]

Las tarjetas inteligentes (ver figura 2.11) proporcionan almacenamiento seguro a prueba de alteraciones para llaves privadas y certificados de seguridad X.509, pueden tener hasta 1 KB de memoria RAM, 24 KB de ROM, 16 KB de memoria ROM programable, 32 ó 64 KB de memoria EEPROM y un procesador de 8 bits que corre a 5MHz, utiliza una interfaz serial y recibe la energía que necesita para funcionar de fuentes externas, como un lector de tarjetas inteligentes.

Dado que el acceso a la información se realiza a través de un puerto serial y supervisado por el propio sistema operativo de la tarjeta, es posible escribir datos confidenciales que no puedan ser leídos por personas no autorizadas. En principio, las funciones de escritura, lectura y borrado de la memoria pueden ser controladas tanto por el hardware como por el software, o por ambos a la vez. Esto permite una gran variedad de mecanismos de seguridad.

Figura 2.11. Tarjeta Inteligente Visa [Visa06B]

a. Ventajas:

- **Seguridad:** El contenido de la banda magnética, por la tecnología que implica, puede ser leído y, aunque no es sencillo, puede ser manipulado por personas con conocimiento y medios adecuados. El chip, sin embargo, contiene una tecnología interna mucho más sofisticada que hace que las posibilidades de manipulación física se reduzcan de forma muy sensible. Además, por su capacidad interna, es capaz de soportar procesos criptográficos muy complejos (DES simple, Triple DES, RSA).

- **Capacidad de almacenamiento de información:** La cantidad de información incorporable a una banda magnética es pequeña y, parcialmente modificable, por lo que la relación entre el usuario de la tarjeta y el emisor es unidimensional: únicamente se actualiza cuando interactúa a través de hardware sofisticado (ATMs). El chip, sin embargo, une a su mayor capacidad de recogida de información, la virtualidad de poder gestionar dicha información, con lo que se abren nuevas posibilidades para la relación usuario-emisor.

- **Flexibilidad:** La tecnología de Tarjetas Inteligentes es compatible con los principales tipos de sistemas operativos. También un entorno de programación que permite crear, almacenar o suprimir aplicaciones en las tarjetas, lo que significa que es posible hacer tarjetas "a medida" seleccionando para la tarjeta las aplicaciones que se adapten a las circunstancias y necesidades de cada persona.

b. Clases de tarjetas inteligentes

- **Tarjeta Inteligente de Contacto:** Estas tarjetas son las que necesitan ser insertadas en una terminal con lector inteligente para que por medio de contactos pueda ser leída. Existen dos tipos de tarjeta inteligente de contacto: Las sincrónicas y las asincrónicas.

Tarjetas Inteligentes Sincrónicas o Tarjetas de Memoria

Los datos que se requieren para las aplicaciones con tarjetas de memoria son almacenados en una EEPROM (Electrical Erasable Programmable Read Only Memory). Estas tarjetas son desechables cargadas previamente con un monto o valor que va decreciendo a medida que se utiliza y una vez que se acaba el monto se vuelve desechable.

Tarjetas Asincrónicas

Estas tarjetas poseen en su chip un microprocesador, y además cuenta con algunos elementos adicionales como son: ROM enmascarada (contiene el sistema operativo de la tarjeta, y se graba durante el proceso de fabricación), EEPROM (es la memoria no volátil del microprocesador, y en ella se encuentran datos del usuario o de la aplicación, así como el código de las instrucciones que están bajo el control del sistema operativo), RAM (es la memoria de trabajo del microprocesador) y Puerto de Entrada/Salida (consiste en un simple

registro, a través del cual la información es transferida bit a bit). El esquema de estas tarjetas se presenta en la figura 2.12:

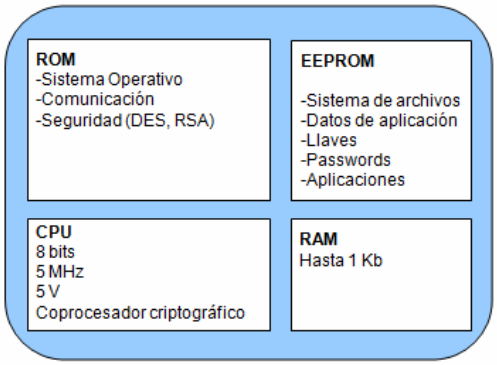


Figura 2.12. Esquemas de Tarjetas Asíncronas

- **Tarjetas Inteligentes sin Contacto:** Son similares a las de contacto con respecto a lo que pueden hacer y a sus funciones, pero utilizan diferentes protocolos de transmisión en capa lógica y física, y el chip se comunica con el lector de tarjetas mediante inducción. Poseen además del chip, una antena de la cual se valen para realizar transacciones. Son ideales para las transacciones que tienen que ser realizadas muy rápidamente.

c. ISO 7816

Es un estándar internacional relacionado con las tarjetas de identificación electrónicas, en especial las tarjetas inteligentes, gestionado conjuntamente por la Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC). Se trata de una extensión de la ISO 7810.

- **ISO 7816-1: Características Físicas:**

  El rasgo más distintivo de una tarjeta es sin duda su aspecto físico. Otra característica notable a simple vista es la presencia o no del área de contactos, que tiene la forma de un cuadrado dorado o plateado, y que se encuentra en la superficie de la tarjeta. En algunos casos esta área no existe (tarjetas sin contacto).

- **ISO 7816-2: Dimensión y localización de los contactos**

  Dado que el microprocesador requiere de una vía por donde tomar la alimentación para sus circuitos o para llevar a cabo la transmisión de datos, es necesaria una superficie física de contacto que haga de enlace entre el lector y la tarjeta.

  Esta superficie consiste en 8 contactos que se encuentran en una de las caras de la tarjeta. El tamaño de los contactos no deber ser nunca inferior a 1,7 mm de alto y 2 mm para el ancho, el valor máximo de estas medidas no está especificado.

  Toda comunicación que se realice con una tarjeta es iniciada siempre por el dispositivo externo, esto quiere decir que la tarjeta nunca transmite información sin que se haya producido antes una petición externa. Esto equivale a una relación maestro-esclavo, siendo el terminal el maestro y la tarjeta el esclavo.

  Cada vez que se inserta una tarjeta en el terminal lector, sus contactos se conectan a los del terminal y éste procede a activarlos eléctricamente; a continuación, la tarjeta inicia un reset de encendido y envía una respuesta llamada ATR (Answer To Reset) hacia el terminal. Esta respuesta contiene información referente a cómo ha de ser la comunicación tarjeta-lector, estructura de los datos intercambiados, protocolo de transmisión y otros

  Una vez que el lector interpreta el ATR procede a enviar la primera instrucción. La tarjeta procesa la orden y genera una respuesta que es enviada hacia el terminal. El intercambio de instrucciones y respuestas acaba una vez que la tarjeta es desactivada.

Los protocolos de transmisión especifican con precisión cómo han de ser las instrucciones, las respuestas a las mismas y el procedimiento a seguir en caso de que se produzcan errores durante la transmisión. Existen alrededor de 15 protocolos distintos, pero dos de ellos son los más utilizados: el T=0 que fue diseñado en 1989, y el T=1 que fue introducido en 1992.

2.1.15 El Estándar EMV (EUROPAY, MASTERCARD AND VISA) [Visa99]

En diciembre de 1993, el grupo EMV –consistente en representantes de Europay, MasterCard y Visa- empezaron a trabajar en el desarrollo de especificaciones para tarjetas chip para la industria mundial, para asegurar que todas las tarjetas chip de débito y crédito puedan operar con todos los terminales lectores de tarjeta, sin importar su ubicación, institución financiera o manufactura. Las especificaciones EMV fueron escritas con los siguientes objetivos:

- La tarjeta y el equipo pueden comunicarse y detectar qué aplicaciones tienen ambas en común.
- El equipo puede correr aplicaciones comunes y asegurar que estándares mínimos de control de riesgo y seguridad son aplicados para las aplicaciones de débito y crédito.
- La experiencia de pago con tarjeta chip conlleva a interoperabilidad y aceptación mundial.

Estas especificaciones proveen un juego de reglas que permiten a la tarjeta chip y al equipo lector comunicarse uno con el otro. Las especificaciones EMV están basadas en un juego de estándares desarrollados por la organización Internacional de Estandarización (ISO) para tarjetas de circuitos integrados y equipos de aceptación relacionados (como equipos POS). Aquí tenemos una serie de normas regulatorias, mostradas a continuación:

- EMV 2000 Versión 4.0 Integrated Circuit Card Specification for Payment Systems. Book 2 Security and Key Management.

- ISO/IEC 10118-3 Information Technology – Security Techniques – Hash Functions – Part 3: Dedicated Hash Functions
- FIPS 140-2:1999 Requirements for Secure Cryptographic Modules
- ISO/IEC 8731-1:1987 Banking-Approved algorithms for message authentication
- ISO/IEC 9564-1:2002 Banking – Personal identification number management and security
- ISO/IEC 11568-1:1994 Banking – Key management (retail) - Part 1:Introduction to key management
- ISO/IEC 11568-4:1994 Banking – Key management (retail) - Part 4:Key management techniques for public key cryptosystems ISO/IEC 11568-5:1994 Banking – Key management (retail) - Part 5:Key life cycle for public key cryptosystems

EMV logra la interoperabilidad entre tarjetas y equipos a través de dos mecanismos. Primero, este define los requerimientos mínimos que las tarjetas chip y los equipos de aceptación de tarjetas deben conocer para comunicarse uno con el otro. Estos requerimientos también aseguran que la tarjeta no sea dañada por el equipo. Luego especifica cómo las transacciones de débito y crédito deben ser ejecutadas, una vez que se ha realizado el contacto físico entre el chip y el equipo. Todos estos requerimientos se definen en los siguientes niveles:

a. Requerimientos EMV Nivel 1

La mayor parte del estándar EMV provee los requerimientos de línea base para todos los chips y terminales, incluyendo características físicas y electromecánicas, interfaz lógica y protocolos de transmisión, para facilitar la interoperabilidad básica. Define los requerimientos esenciales que permiten que las tarjetas con chip y terminales se comuniquen unos con otros. Esto asegura que una tarjeta EMV insertada en un Terminal Nivel 1 nunca dañará al Terminal ni viceversa.

Específicamente, la tarjeta y el equipo deben estar habilitados para conectarse físicamente para permitir el intercambio de información. Desde la perspectiva de tarjeta, el tamaño de la tarjeta, la posición del chip, y los contactos del chip deben seguir las especificaciones de EMV. Desde la perspectiva del equipo, el terminal debe contar con el correcto tamaño de slot para encajar la tarjeta y sus contactos deben estar en la posición correcta para hacer contacto físico con el chip de la tarjeta.

EMV también especifica el voltaje que el equipo debe aplicar al chip para alimentarlo con el poder que necesita para participar en una transacción. Los demás requerimientos incluyen protocolos de comunicación para transmitir datos entre la tarjeta y el equipo, la secuencia de envío de caracteres y el número de caracteres a enviar por vez.

b. Requerimientos EMV Nivel 2

El resto de estándares EMV define los requerimientos (selección de aplicaciones, elementos de datos, comandos, aspectos de seguridad, otros) para la ejecución de funciones asociadas con transacciones de débito y crédito.

Una vez que la conexión ha sido establecida, EMV especifica un mecanismo que permite a la tarjeta y al equipo determinar si existe o no alguna razón para continuar con la transacción. El equipo extrae información de la tarjeta sobre la aplicación POS contenida en él (ver figura 2.13), basado en las preferencias del tarjetahabiente y decide la aplicación a ser usada en la transacción. Esta decisión hecha proceso es llamada selección de aplicación. En otras palabras, luego que un tarjetahabiente inserta una tarjeta chip, el equipo generará una lista de aplicaciones contenidas tanto en la tarjeta como en el terminal y las presenta al tarjetahabiente para su selección.

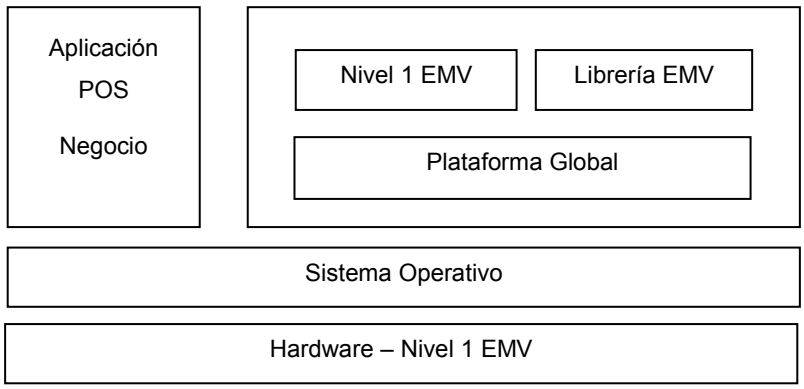


Figura 2.13. Composición interna de tarjetas Chip

2.1.16 Módulo de Seguridad Resistente a Alteraciones

Un Módulo de Seguridad Resistente a Alteraciones (comúnmente conocido como TRSM) debe cumplir los requisitos de un Dispositivo Físicamente Seguro según se definen en la norma ISO 9564–1. Este tipo de dispositivo ofrece una mínima probabilidad de ser penetrado para divulgar la totalidad o una parte de cualquier clave criptográfica o PIN. El TRSM se puede certificar solamente después que se haya determinado que la operación interna del dispositivo no ha sido modificada para permitir su penetración (es decir, la introducción en el dispositivo de un mecanismo activo o pasivo de vigilancia). Provee facilidades y funciones criptográficas necesarias para asegurar transacciones en redes financieras y/o bancarias.

Se consideran los dos tipos siguientes de Módulos de Seguridad Resistentes a Alteración:

- Dispositivos receptivos o físicamente seguros contra alteraciones: La penetración del dispositivo causará que se borren inmediatamente todos los PINs, llaves criptográficas y todos los residuos útiles de PINs y llaves contenidas en los mismos.
- Dispositivos donde la alteración es evidente o equipos de ingreso de PIN aceptables que cumplen con las normas mínimas: cualquier intento de penetrar el dispositivo será obvio. Este tipo de dispositivo sólo se puede usar

para esquemas de encriptación de PIN y administración de llaves donde la penetración del dispositivo no ofrezca información sobre los PINs o llaves secretas que se hayan ingresado previamente.

HSM 8000 – Host Security Module

El HSM 8000 (ver figura 2.14) es un equipo resistente a alteraciones que provee facilidades criptográficas necesarias para asegurar las transacciones en redes financieras. Este equipo es usado generalmente para validar la información de los canales POS y ATM. Algunas de sus características se describen a continuación:

- Soporta funciones de verificación de tarjeta y PIN de tarjetas Visa, MasterCard, American Express y otras.
- Soporta el estándar EMV 3.1.1 y EMV 4.0, procesamiento de transacciones y aseguramiento de mensajería bajo estos estándares.
- Carga de llaves de manera remota para cajeros NCR y Diebold.
- Esquemas de transacciones de llaves DES, Triple DES y DUKPT.
- Generación, carga y verificación de llaves RSA, con longitudes desde 320 a 2048 bits, generación y validación de firmas digitales.
- Componentes de Llave Maestra Local almacenadas en Smart Cards, generadas bajo el ISO 7816, para su almacenamiento seguro y distribución.
- Interfaces de comunicación TCP/IP y UDP, Ethernet 10/100 Base T, asíncrona, RS232 y SNA.
- Utiliza el Subsistema Genérico Seguro Thales (Thales Secure Generic Sub-system SGSS) para todo el procesamiento de seguridad y criptografía, el cual es validado por FIPS 140-1 Nivel 4 y FIPS 140-2 Nivel 2.

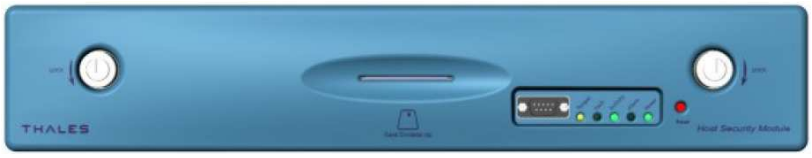


Figura 2.14. HSM 8000 [Thales04]

FIPS PUB 140-1 Security Requirements for Cryptographic Modules

Especifica los requerimientos de seguridad que deben ser satisfechos por el módulo criptográfico utilizado entre un sistema de seguridad para la protección de información sensible, con computadoras y sistemas de telecomunicaciones. También contempla los puertos e interfaces de comunicación del módulo, autenticación, servicios, roles, seguridad física, ambiente operacional, administración de llaves, compatibilidad e interferencia electromagnética, pruebas internas, diseño y mitigación de ataques.

El estándar provee cuatro incrementales y cualitativos niveles de seguridad, que intentan cubrir los diferentes ambientes en los que un módulo de seguridad puede ser utilizado.

- Nivel 1: nivel más bajo que establece requerimientos básicos, como algoritmos aprobados por FIPS. No se requieren mecanismos físicos muy limitados para módulos en producción, eliminando las vulnerabilidades de seguridad más resaltantes.
- Nivel 2: añade requerimientos para evidencia de alteración física o uso de coberturas para evitar accesos no autorizados, autenticación basada en roles
- Nivel 3: añade requerimientos para evitar alteraciones, como cierre hermético, que al detectar que el equipo ha sido alterado de manera física, borre los parámetros de seguridad automáticamente. Provee autenticación basada en identidad. Los puertos de configuración de parámetros de seguridad críticos deben estar físicamente separados de los puertos para el ingreso de los demás datos. Estos parámetros sólo podrán ser manipulados por otras aplicaciones de manera encriptada o ser ingresados directamente en el módulo.
- Nivel 4: este nivel permite detectar la penetración en el equipo de manera lógica. El modo de operación de los equipos debe ser bajo control dual y conocimiento compartido. Detecta cambios ambientales, de temperatura, de movimiento o de voltaje, y borra los parámetros de seguridad cuando esto ocurre.

FIPS PUB 140-2 Cryptographic Module Validation Program (CMVP)

Programa de acreditación de seguridad de tecnologías de información para módulos criptográficos producidos por vendedores del sector privado que buscan contar con productos certificados para su uso en departamentos de gobierno y entidades reguladas (instituciones financieras y de cuidado de la salud) que colectan, almacenan, transfieren comparten y distribuyen información sensible y/o clasificada.

- Nivel 1: nivel más bajo que establece pocos requerimientos muy limitados para módulos en producción, eliminando las vulnerabilidades de seguridad más resaltantes.
- Nivel 2: añade requerimientos para evidencia de alteración física y autenticación basada en roles.
- Nivel 3: añade requerimientos para resistencia de alteración física y autenticación basada en identidades, y para la separación lógica y física entre las interfaces que ingresan parámetros de seguridad críticos y otras interfaces.

  Todas las claves DES utilizadas para encriptar las claves para su transmisión deberán ser al menos claves de longitud doble y usar el TDEA en un modo de operación de encriptación o desencriptación de clave. No se deberá encriptar una clave DES de longitud triple con una clave DES de menor longitud.

  Las Claves de Archivo Maestro del Módulo de Seguridad, incluyendo las generadas internamente al HSM y nunca exportadas, deben ser claves de longitud doble que usen el TDEA.
- Nivel 4: este nivel hace los requerimientos de seguridad física más severos y los requerimientos más robustos contra ataques ambientales.

2.1.17 Cajero Automático

Automatic Teller Machine (ATM), es un dispositivo de las entidades bancarias al que pueden dirigirse sus clientes a cualquier hora para realizar operaciones de retiro, transferencias o consulta. Se trata de máquinas conectadas a una central mediante redes de comunicación, y a las que se tiene acceso a través de una tarjeta de identificación personal, con banda magnética o chip que contiene el número de tarjeta y otra información de seguridad, como la fecha de expiración y el CVV. La identificación del usuario es a través del Número de Identificación Personal (PIN).

La información ingresada por el usuario y leída de la tarjeta, es encriptada por el ATM, para ser enviada a la entidad correspondiente para su validación. Así mismo, el ATM desencripta la información que le es enviada desde el servidor correspondiente.

2.2 Marco Conceptual

- Administración de llaves criptográficas: actividades relacionadas con el manejo de las llaves criptográficas y otros parámetros de seguridad relacionados con las mismas durante todo el ciclo de vida de las llaves, incluyendo su generación, almacenaje, distribución, carga y uso, eliminación, destrucción y archivo.
- Aleatorio: El proceso de generar valores con un alto nivel de entropía y que satisfacen diversas calificaciones, utilizando mecanismos criptográficos y de hardware basados en "ruido". Esto trae como resultado un valor en un conjunto que tiene iguales probabilidades de ser seleccionado del total de posibilidades, es decir, que es impredecible.
- Algoritmo criptográfico: una serie de reglas, configuradas a través de procedimientos necesarios para autenticar o proteger datos.
- ATM: o cajero automático.
- Carga de llaves: Proceso mediante el cual se transfiere una llave manual o electrónicamente a un dispositivo criptográfico seguro.

- Componente de llave: uno de al menos dos parámetros que tienen las características de aleatoriedad y formato de una llave criptográfica que es combinada con uno o más parámetros similares formando una llave criptográfica.
- Conocimiento compartido: Una condición bajo la cual dos o más entidades separadamente tienen componentes de llave que individualmente no transmiten ningún conocimiento de la llave criptográfica resultante.
- Consola: estación de trabajo que se conecta a los HSM para poder tener acceso a la configuración de sus funcionalidades o a operaciones con llaves criptográficas.
- Control dual: proceso de utilización de dos o más entidades separadas para proteger información sensible o funciones, para que una sola entidad no esté habilitada para acceder o utilizar dicha información o funciones.
- Criptografía: el proceso que transforma los datos para garantizar su origen, la conciliación del contenido de su información, prevención contra modificación no detectada, prevención de uso no autorizado, prevención de repudio, o cualquiera de sus combinaciones.
- Custodio: persona a la que se le asigna el resguardo de la confidencialidad de una llave, componente de llave o llave física.
- Desencriptar: El proceso de transformar el texto cifrado (que no se puede leer) a texto sin cifrar o sin formato, es decir, en texto en claro (legible).
- Encriptar: transformación (reversible) de datos por medio de un algoritmo criptográfico para producir un texto cifrado; es decir, para ocultar la información que contienen los datos.
- Equipo criptográficamente seguro: un equipo que provee almacenamiento seguro para información secreta como llaves y servicios de seguridad basados en información secreta.
- Firma digital: transformación criptográfica de datos que, cuando es implementadas apropiadamente provee autenticación de origen integridad de datos y no-repudio del firmante.
- Franquicia: Acuerdo de venta en el que una compañía (franquiciador) cede los derechos a una persona o compañía (franquiciatario) para proporcionar los productos o servicios del franquiciador en un mercado específico. El franquiciatario

se compromete a operar de acuerdo a las normas establecidas por franquiciador, las cuales normalmente incluyen el uso de sus productos, materiales promocionales y otros servicios de soporte de la compañía. En contraprestación, el detallista (franquiciado) paga una cuota de entrada, abona un porcentaje de los ingresos y acepta las condiciones de venta que se le imponen.

- HSM: hace referencia a ambos equipos HSM, principal y de respaldo instalados en el Banco de la Nación. Cuando se requiera hacer diferenciación de los mismos se referencia como HSM Principal o HSM 1, a aquel instalado en la Oficina Principal. Así mismo, se llamará HSM de Respaldo o HSM 2, a aquel instalado en la Oficina de Respaldo.
- Llave criptográfica: conjunto de números hexadecimales utilizados para mantener la confidencialidad e integridad de información privada. También será referenciado como clave criptográfica o llave.
- Llave criptográfica: un parámetro que define la operación de un algoritmo criptográfico.
- Número de Identificación personal: Un código de identificación personal que autentica a un tarjetahabiente en una solicitud de autorización que se origina en un terminal con capacidad de autorización solamente o captura de datos solamente. Un PIN consiste en dígitos decimales solamente.
- Switch Central de ATMs: es el switch que conecta a todos los ATMs entre sí. Este término hace referencia a ambos switch (principal y respaldo). También será referenciado pro su marca Switch Stratus.
- Tarjeta chip, tarjeta IC o ICC: tarjeta con un chip embebido, de débito o crédito, que cuenta con un circuito integrado, conocido también como chip o IC (por sus siglas en inglés Integrated Circuit). También referenciado como tarjeta inteligente o Smart Card (en inglés).
- Tarjetahabiente: persona a quien se emite una tarjeta o que está autorizada para usar la tarjeta.
- Token: tarjeta inteligente utilizada por un custodio de componente de clave criptográfica, para resguardar la seguridad de dicho componente.

- Valor de Verificación: El valor de computación que resulta al pasar los datos a través de un algoritmo irreversible. Los valores de verificación generalmente se calculan utilizando una transformación criptográfica que usa una clave secreta y una cadena arbitraria para la transformación criptográfica y que da un valor de verificación criptográfico como resultado. La computación de un valor de verificación correcto no será posible sin conocer la clave secreta.

Capítulo 3: Estado del Arte

Aquí se describe la situación actual de los algoritmos criptográficos relacionaos al problema y a la solución, así como la infraestructura criptográfica actual del Banco de la Nación basado en los conceptos descritos en el Marco Teórico y Conceptual.

3.1 Taxonomía de algoritmos criptográficos

La elección de un algoritmo puede ser hecha de acuerdo a su funcionalidad, técnica, legalidad o aspectos comerciales. Esto puede ser útil para proponer una taxonomía de algoritmos criptográficos basados en diferentes criterios. Aquí se propone clasificar los algoritmos de acuerdo a sus:

- Características técnicas
- Uso típico
- Estado comercial o legal
- Dominio de aplicación [ECBS03]

Esta taxonomía nos servirá para clasificar el algoritmo DES, el cual es el que actualmente se utiliza en el Banco de la Nación y es tema de estudio.

3.1.1 Características técnicas

- Simétrica (cifradores de cadena y de bloque)
- Asimétrica (también conocido como algoritmos de llaves públicas)
- Funciones hash
- Otros (DUKPT, Diffie Hellman)

La figura 3.1 propone una taxonomía de primitivas y mecanismos criptográficos basados en sus características técnicas. Algoritmos usados comúnmente ordenados de acuerdo a esta taxonomía son dados como ejemplos:

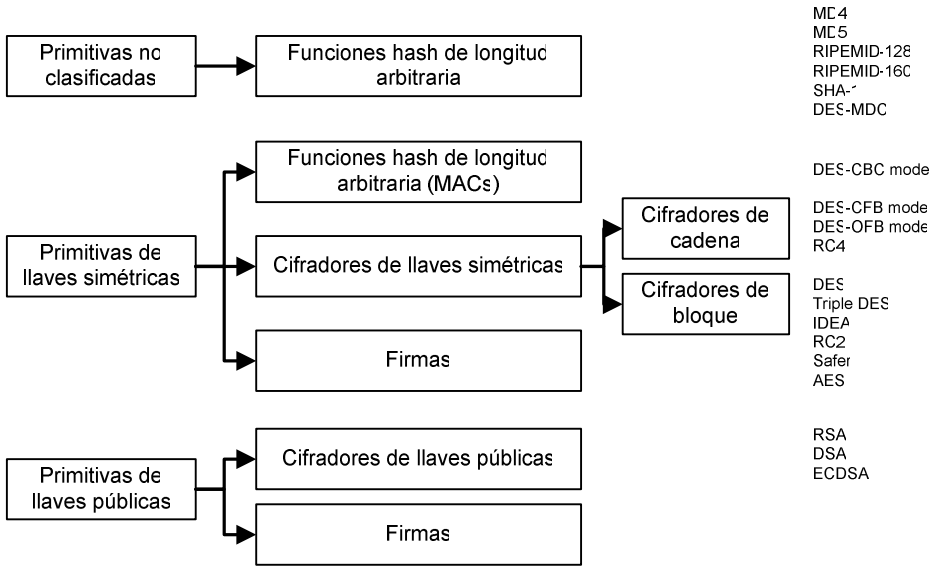


Figura 3.1. Una taxonomía técnica de primitivas y mecanismos criptográficos [ECBS03]

- Las funciones de llaves (también conocidas como Código de Autenticación de Mensajes MAC) son usualmente algoritmos simétricos usados como llaves secretas: típicamente DES usadas en modo CBC.
- Funciones Hash no clasificadas pueden ser:
  - Funciones Hash específicas sin ninguna clase de llaves, como funciones derivadas de MD4, MD5, SHA-1, RIPEMD, o funciones basadas en aritmética modular.
  - Algoritmos simétricos donde la llave requerida por el algoritmo no es secreta y puede ser reemplazada por datos que están siendo protegidos: típicamente DES usado en modo MDC.
- Usualmente cifradores de cadena son usados en la implementación de hardware para aplicaciones de telecomunicaciones. Usualmente son algoritmos propietarios y sus especificaciones son confidenciales. Pocos estándares internacionales están disponibles en este tema.
- Los cifradores en bloque podrían ser usados de acuerdo a los diferentes modos de operación. Los modos de operación mejor conocidos son aquellos cifradores simétricos en bloque como el DES.

3.1.2 Uso típico

- Autenticación del origen de los datos
- Autenticación de entidad
- Confidencialidad de datos
- Confidencialidad de llaves
- Integridad de datos
- Establecimiento de llaves
- No repudio

La siguiente tabla muestra qué clase de técnica criptográfica es considerada adecuada para un uso específico:

Características técnicas Uso	Simétricas	Asimétricas	Funciones Hash no clasificadas
Autenticación del origen de los datos(6)	Sí (uno a uno)(1)	Sí (uno a muchos)	Sí(3)
Autenticación de entidad	Sí(uno a uno)	Sí(uno a muchos)	No
Confidencialidad de datos	Sí	No(4)	No
Confidencialidad de llaves	Sí	Sí(4)	No
Integridad de datos	Sí(1)	Sí(5)	Sí
Establecimiento de llaves	No	Sí	No
No repudio	No	Sí(2)	Sí, como entrada(3)

Tabla 3.1. Comparación de técnicas y funcionalidades de seguridad [ECBS03]

1. Cuando un algoritmo simétrico es usado para calcular el MAC, tanto la autenticación de datos de origen e integridad son provistos.
2. Algoritmos asimétricos basados en firmas pueden soportar el servicio de no repudio si se usa en un contexto legal apropiado.
3. Una función hash no clasificada es designada básicamente para proveer integridad de datos. Es usualmente usado como un componente de un esquema de firma digital. En este caso el hash es transformado por un algoritmo asimétrico usando las llaves privadas.
4. Algunos algoritmos asimétricos proveen confidencialidad, pero el proceso de descripción requiere una largo tiempo de procesamiento. Consecuentemente, esta propiedad es usada sólo cuando la performance no es tan crítico como la

confidencialidad de la llave (para transporte de llaves simétricas). En algunos países, su uso para confidencialidad de datos pueden también ser restringidos por regulación nacional.

5. Cuando es usado para computar firmas digitales, los algoritmos asimétricos proveerán integridad como un producto del proceso de firma.
6. La autenticación del origen de los datos implica integridad de datos. [ECBS03]

3.1.3 Estado comercial o legal

Los algoritmos pueden ser clasificados de acuerdo a su estado comercial o legal en:

- Reservado para el uso del gobierno
- Estándar De jure o de facto
- Algoritmo propietario
- Patentado o disponible público

Los algoritmos reservados para el uso del gobierno son usualmente mantenidos en secreto. Puede suceder que los gobiernos excepcionalmente autoricen a compañías comerciales a usar dichos algoritmos. Bajo estas circunstancias los usuarios deben estar enterados tanto de las especificaciones técnicas del algoritmo como de que éstos no sean hechos públicamente disponibles, que no pueden ser sometidos a investigación de expertos criptoindependientes y consecuentemente su longitud no puede ser fijada.

Por otro lado, en algunos países el uso de técnicas criptográficas para confidencialidad es restringido por el gobierno.

Algunos algoritmos han sido estandarizados por la ISO (usualmente por ISO/IEC, JTCI/SC27 o ISO TC68/SC2) o por organismos americanos como

ANSI, o son estándar de jure (de derecho o legal). Otros algoritmos nunca han sido estandarizados, pero son reconocidos por la industria como estándar de facto (o de hecho), por ejemplo RSA PCKS. ISO también mantiene un registro de los algoritmos criptográficos. El algoritmo DES pertenece a esta clasificación al estar normado por dichos organismos internacionales.

Los algoritmos propietarios son usualmente encontrados en hardware criptográfico (cajas de encripción o tarjetas inteligentes). Sus especificaciones son mantenidas en secreto como algoritmos reservados para el uso del gobierno.

Los algoritmos RC2, RC4 y RC5 los cuales son ampliamente usados en SSL o S/MIME son algoritmos propietarios desarrollados por RSA Data Security Inc.

La seguridad de la criptografía moderna depende del acceso público al algoritmo y el secreto de la llave criptográfica. Los algoritmos son típicamente publicados y han sido extensivamente estudiados por los criptógrafos. El algoritmo DES por ejemplo, ha sido publicado en varios estándares y otros documentos. El algoritmo RSA está basado en principios matemáticos ampliamente conocidos. La seguridad operacional de estos algoritmos criptográficos depende enteramente de que tan bien las llaves secretas y privadas han sido administradas durante todo su ciclo de vida. [ECBS03]

3.1.4 Dominio de Aplicación

Los algoritmos pueden ser clasificados de acuerdo a su dominio de aplicación por el cual fueron designados o por el cual pueden ser mejor clasificados. Estos dominios pueden ser:

- Home Banking
- Transacciones en línea – ventas (generación o verificación de PIN)
- Transacciones en línea – host o host
- Transferencia batch de transacciones individuales

- Transferencia de archivos (EDI)
- Correo electrónico
- Bolsa electrónica
- Tarjetas de débito o crédito
- Respaldo seguro
- Otros

Cuando el dominio de la aplicación es concerniente, criterios típicos pueden ser usados para seleccionar el algoritmo más apropiado y el esquema de administración de llaves puede ser:

- Performance esperada, incluyendo el tiempo de respuesta en sistemas interactivos
- Volumen de datos a proteger
- Administración de llaves apropiado para un grupo de usuarios abierto o cerrado
- Necesidad de una tercera parte confiable
- Escalabilidad
- Costos, para configurar el sistema y mantenerlo andando
- Sensibilidad percibida de los datos a proteger
- Requerimientos de qué tanto tiempo de protección en necesario [ECBS03]

3.2 Estructura de Llaves Criptográficas del Banco de la Nación

El Banco de la Nación, para la implementación de las tarjetas Multired Global Débito, así como para la certificación en el Rol Adquirente para los cajeros automáticos, estableció una estructura tecnológica para soportar un esquema de llaves criptográficas que se encuentre basado en el algoritmo DES. Esta estructura se muestra a continuación:

3.2.1 Llave Maestra – Local Master Key (LMK)

Esta llave criptográfica es única por institución y por módulo criptográfico. A partir de ella se deben generar las llaves KEK y de trabajo distintas por cada canal de atención. Es la llave bajo la cual se generarán todas las demás llaves con las que la institución trabaja. Esta llave se encuentra almacenada en los equipos HSM pero de manera encriptada. Sólo es posible visualizar su generación a partir de su valor de chequeo, ya que no es permitido visualizar el valor encriptado de la llave.

Esta llave es generada a partir de tres (3) componentes. Los equipos HSM soportan la generación de la LMK de 2 a 9 componentes y los almacena en Smart Cards, las cuales son manejadas por diferentes custodios.

Cada componente de la LMK puede contar con una copia. Esta copia es generada por el custodio suplente desde el HSM y almacenada en una ubicación física distinta a la de la Smart Card titular.

Adicionalmente, y como medida de seguridad de los HSM, las funciones relacionadas a la LMK están sujetas a una validación adicional. Para tener acceso a la generación de componentes de LMK, a su modificación, restauración o eliminación, será necesario el uso de dos llaves físicas, las cuales deben ser ingresadas al HSM para desbloquear dichas funciones.

3.2.2 Llaves de Encripción de Llaves – Key Encrypting Key (KEK)

Son llaves generadas directamente a partir de la LMK, y son utilizadas para generar llaves de trabajo.

3.2.2.1 Zone Master Key (ZMK)

Es una llave utilizada para intercambiar información entre dos entidades. En los casos en que dos organizaciones compartan una clave

para encriptar PIN y se la comuniquen entre sí, dicha clave deberá ser única para esas dos organizaciones y no se le deberá dar a ninguna otra organización. Esta técnica de utilizar claves únicas para la comunicación entre dos organizaciones se conoce como "zone encryption" o "encriptación por zona". Las claves pueden existir en más de un par de ubicaciones para fines de recuperación en caso de desastre o balance de carga (por ejemplo, ubicaciones de procesamiento dual).

La ZMK se genera en el HSM a partir de dos (2) o más componentes. En la interconexión con Visa, es necesario que se manejen tres (3) componentes para generar la ZMK.

3.2.2.2 Terminal Master Key (TMK)

Es la llave inscrita en un terminal ATM a partir de la cual se generan las llaves de trabajo que encriptan y validan la información que ingresa a través de un terminal.

Esta llave se genera en el equipo HSM a partir de dos (2) componentes custodiados por dos personas diferentes, luego de lo cual dichos componentes deben ser inscritos en claro en el terminal (en este caso en el cajero automático) y su valor encriptado en el switch central ATM, según podemos apreciar en la figura 3.2:

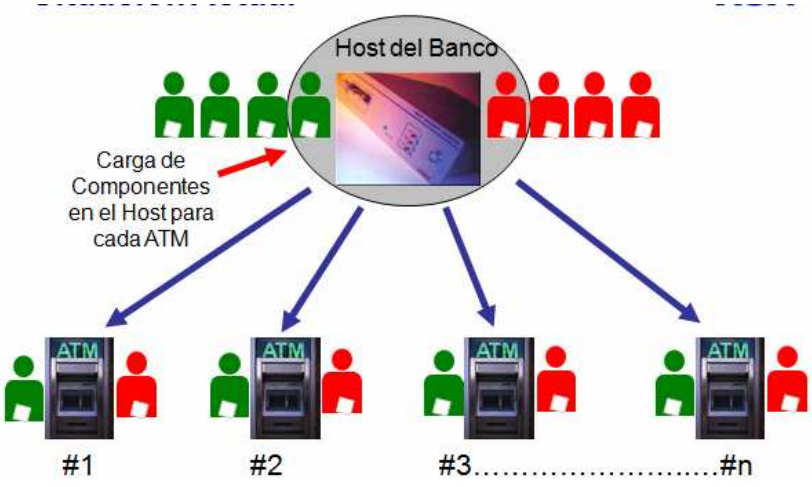


Figura 3.2. Carga de componentes en cada ATM [Visa06B]

3.2.3 Llaves de Trabajo – Working Key

Son las llaves generadas a partir de llaves KEK y que se utilizan directamente para encriptar la información crítica que se desea proteger.

3.2.3.1 Card Verification Key (CVK)

Es la Llave de Verificación de Tarjeta, con el cual se genera y valida el CVV (Card Verification Value) que se encuentra inscrito en la banda magnética. Existen dos claves que componen la CVK: CVK_A y CVK_B, las cuales son utilizadas en el mismo proceso de generación del CVV, para encriptar (CVK_A), desencriptar (CVK_B) y luego encriptar (CVK_A) los datos que generan el CVV, como vemos en la siguiente figura:

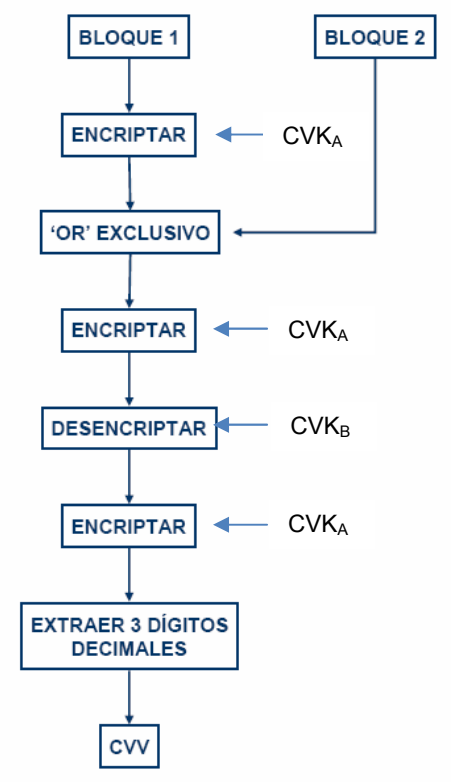


Figura 3.3. Esquema de generación de CVV [Thales05]

Se concatenan los bits del número de cuenta, fecha de expiración y código de servicio. Este bloque de datos se divide en dos bloques de 64 bits, completando a la derecha con ceros binarios según sea necesario. Luego el bloque izquierdo es el bloque 1 y el bloque derecho es el bloque 2.

El CVV es un código de tres dígitos que se encuentre grabado en la banda magnética, se genera en el cajero automático a partir de los datos de la tabla 3.1, y viaja a través de la red hacia el emisor en el PIN Block.

DATOS	COMPOSICIÓN
CVK A	Clave DES de 64 bits – 16 dígitos hexadecimales
CVK B	Clave DES de 64 bits – 16 dígitos hexadecimales
Número de cuenta	Número variable de dígitos
Fecha de expiración	4 dígitos
Código de servicio	3 dígitos

Tabla 3.2. Datos de composición del CVV [Thales05]

3.2.3.2 PIN Verification Key (PVK)

Es la Llave de Verificación de PIN, con el cual se genera y valida el PVV (PIN Verification Value). Existen dos claves que componen la PVK: PVK_A y PVK_B, las cuales son utilizadas en el mismo proceso de generación del PVV, para encriptar (PVK_A), desencriptar (PVK_B) y luego encriptar (PVK_A) los datos que generan el PVV, como vemos en la siguiente figura:

Figura 3.4. Esquema de generación de PVV [Thales05]

El PVV es un código de 4 dígitos que se genera en el cajero automático a partir del valor PIN ingresado y llave PVK correspondiente, y viaja a través de la red hacia el emisor en el PIN Block. Estos datos utilizados para formar el PVV se llaman TSP (Transformed Security Parameter).

Cabe resaltar que el PVV se compara con el PVV inscrito en la Base de Datos del Emisor, nunca se compara con el valor del PIN directamente, ya que este valor nunca se almacena en la Base de Datos.

PVKI - PIN Verification Key Index – Índice de la Llave de Verificación del PIN:

Se pueden utilizar diferentes pares de PVK para un grupo de tarjetas. El PVKI indica el par de llaves PVK que se utiliza para una determinada tarjeta. El PVKI puede variar entre 1 y 6.

3.2.3.3 Zone PIN Key (ZPK)

Llave PIN de zona, encriptada bajo la ZMK. Se utiliza para cifrar la información que viaja entre el banco y Visa. Aquí existen dos tipos de llaves: la IWK y AWK. Ambas se encuentran inscritas tanto en el switch del banco como en el de Visa. Pueden ser generadas In-home y luego remitidas de manera encriptada a Visa, como también pueden ser solicitadas a Visa para que sean desencriptadas e inscritas en el switch del Banco.

- IWK (Issuer Working Key): Llave de trabajo de Emisor, utilizada para enviar transacciones foráneas hacia la nube Visa.
- AWK (Acquirer Working Key): Llave de trabajo de Adquiriente, utilizada para recibir transacciones foráneas desde la nube Visa.

En la figura 3.5 se muestra la relación entre la ZMK y ZPK, en su intercambio entre el Emisor o Adquirente, y un punto de comunicación de Visa Internacional o con Visanet Perú.

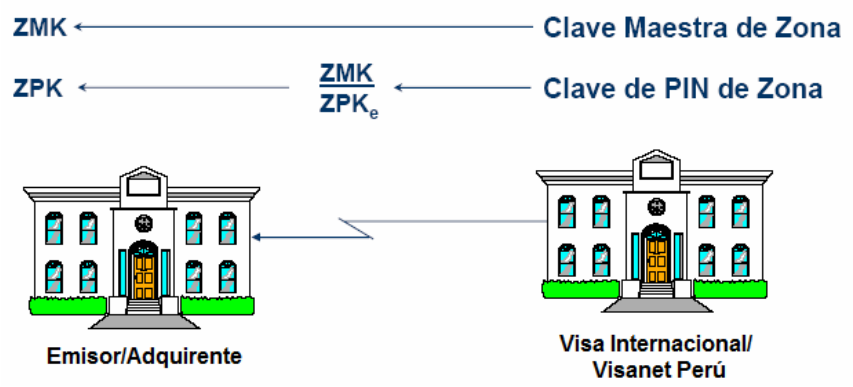


Figura 3.5. Relación entre las llaves ZMK y ZPK [Thales05]

3.2.3.4 Terminal PIN Key (TPK)

Llave PIN de terminal, la cual es generada de manera dinámica desde los equipos HSM a partir del valor de la TMK, de acuerdo al número de transacciones realizadas en el cajero, al número de PIN ingresado erróneamente, o al tiempo transcurrido. Como podemos ver en la figura 3.6, esta llave cifra la información que se ha generado para formar el PIN Block y la envía al switch central ATM de la entidad Adquirente,

que descifra la información y de ser el caso, la envía a la entidad Emisora a través de la conexión con Visa.

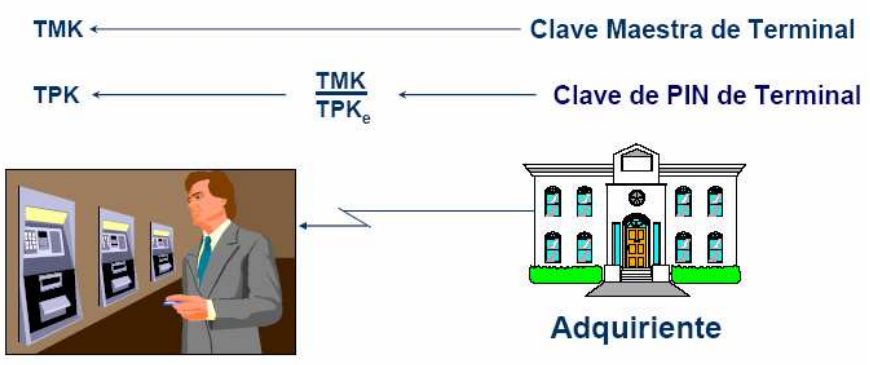


Figura 3.6. Relación entre las llaves TMK y TPK [Thales05]

En la figura 3.7, podemos apreciar la interacción final entre ZMK, ZPK, TMK y TPK, considerando a las entidades emisoras, adquirentes y el switch de Visa Internacional:

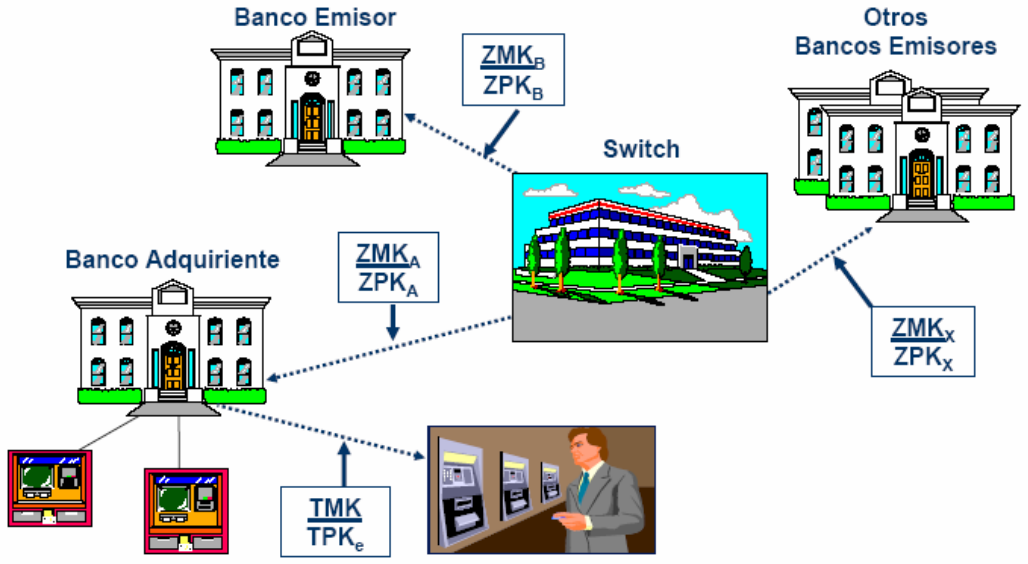


Figura 3.7. Relación de ZMK, TMK, Adquirente y Emisor [Thales05]

3.2.3.5 Message Authentication Code (MAC)

Código de Autenticación de Mensaje, es una llave generada de acuerdo al tipo de transacción a partir de información no confidencial. Valida que la información recibida es auténtica.

3.2.4 Valor de Chequeo

Es un valor generado a partir del texto en claro, ya sea de una llave o componente de llave criptográfica, y del valor de la LMK. A un componente en claro o llave criptográfica en claro le corresponde un y sólo un valor de chequeo, por lo cual sirve para verificar que una llave o componente de llave criptográfica ha sido ingresada de manera correcta.

3.2.5 PIN Block

Es un bloque de datos en el cual se encuentra inscrito el PVV, CVV, el número de cuenta, datos de la transacción y otros datos de la banda magnética. El PIN Block viaja cifrado bajo la TPK inscrita en el cajero automático en el cual se realizó la transacción.

3.2.6 Esquema de validación actual

El esquema tecnológico utilizado actualmente por el Banco de la Nación se muestra en la figura 3.8. Cabe resaltar que esta infraestructura es idéntica en la Oficina principal y en la Oficina de Respaldo. Estas oficinas se comunican a través de una conexión directa entre los computadores centrales IBM.

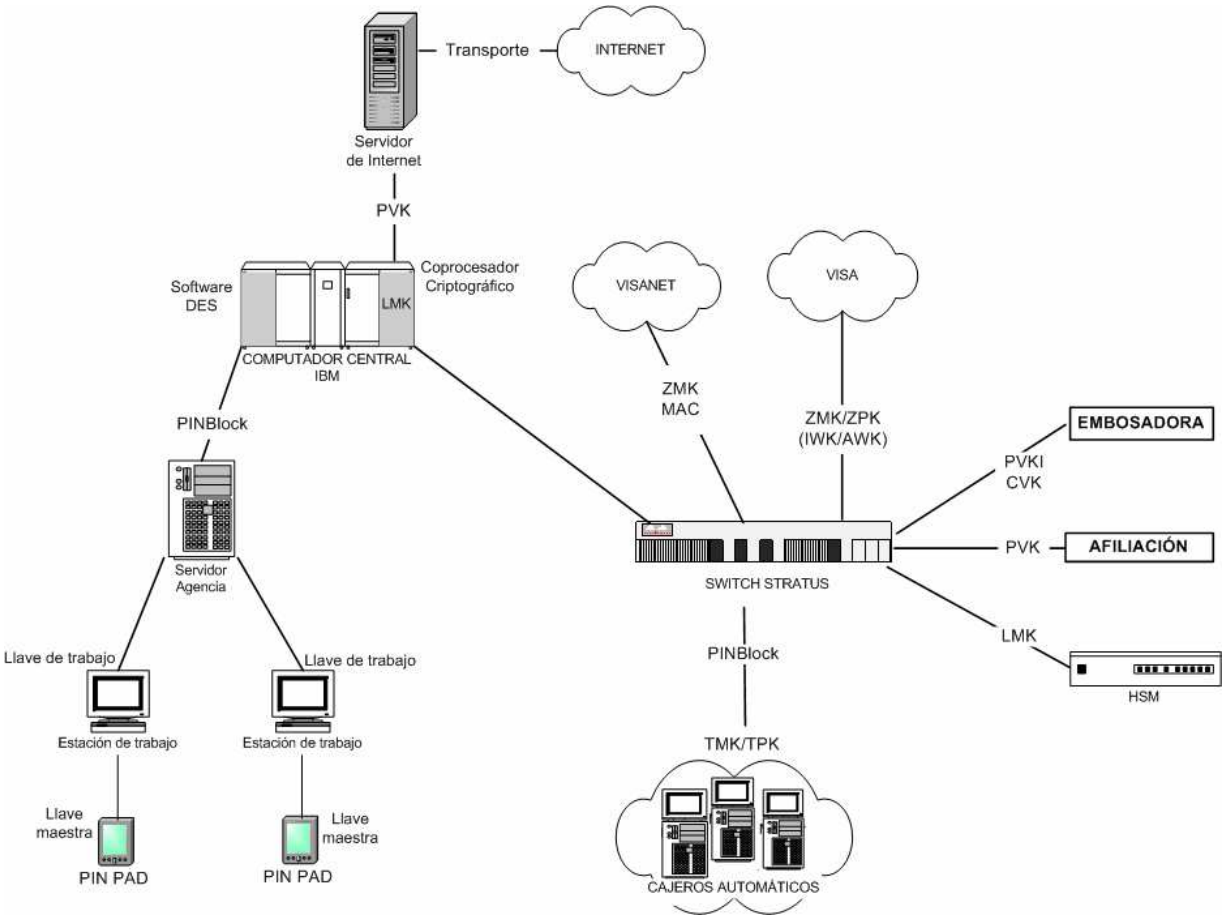


Figura 3.8. Esquema de conexión interna actual [BNSI07]

A continuación se describe el modo de funcionamiento:

a. Switch Stratus

- Es el modelo del switch central de los ATMs del Banco de la Nación, a donde llega toda la información de las transacciones de los cajeros automáticos.
- Aquí se encuentran inscritas los valores encriptados generados por los HSM y/o el coprocesador criptográfico.

b. Generación de tarjetas

- Se inicia en el Computador Central (modelo z-Series 890), donde se genera un archivo de generación de tarjetas nuevas que es enviado al

Switch Central de ATM, o conocido como su nombre comercial Switch Stratus.

- El Switch Central ATM envía dicho archivo con las claves CVK y PVK asociadas a las tarjetas respectivas a la embosadora.
- Cada tarjeta generada no contiene ningún PIN asociado, ya que éste no se genera hasta su afiliación en ventanillas.
- Se almacena en la pista 1 también el valor PVKI correspondiente.

c. Afiliación de tarjetas

- Cuando se asocia una tarjeta nueva a un cliente en una ventanilla del Banco de la Nación, se le asocia un PIN, se genera el PVV, de acuerdo al valor PVKI asociado, a través de la PVK; y se almacena en la Base de Datos del Banco de la Nación.

d. Transacción en cajero automático de la red Multired

- Transacción On-Us (rol emisor): cuando una tarjeta Multired Global Débito realiza una transacción en un cajero de la red Multired, los datos del PIN Block generados bajo la TPK son enviados al Switch Central ATM y validados por el computador central del banco. Aquí se validan los datos de la transacción y de la tarjeta y envía el mensaje correspondiente al cajero automático.

- Transacción doméstica (rol adquirente): cuando un cliente de otro banco del Perú, con tarjeta Visa, realiza una transacción en un cajero de la red Multired. El PIN Block generado bajo la TPK, llega al switch central ATM y es identificada como transacción doméstica. El Switch Central envía el PIN Block a la nube VisaNet Perú, encriptado bajo la ZMK Visanet, y VisaNet Perú la envía a la entidad emisora correspondiente con el MAC calculado. Una vez resuelta la transacción por la entidad emisora, envía la respuesta a través de la nube VisaNet Perú, al switch

central ATM y finalmente al cajero automático, con la respuesta al cliente.

- Transacción internacional (rol adquirente): cuando un cliente de otro banco no perteneciente a Perú, con tarjeta Visa, realiza una transacción en un cajero de la red Multired. El PIN Block generado bajo la TPK, llega al switch central ATM y es identificada como transacción internacional. El Switch Central envía el PIN Block a la nube Visa, encriptado bajo la IWK, y Visa la envía a la entidad emisora correspondiente. Una vez resuelta la transacción por la entidad emisora, envía la respuesta a través de la nube Visa, al switch central ATM y finalmente al cajero automático, con la respuesta al cliente.

e. Transacción en cajero automático de la red Visa

- Transacción doméstica (rol emisor): cuando un cliente del Banco de la Nación con tarjeta Multired Global Débito, realiza una transacción en un cajero Visa de Perú. El PIN Block generado bajo la TPK, llega al banco y es identificada como transacción doméstica. El Banco envía el PIN Block a la nube VisaNet Perú, encriptado bajo la ZMK Visanet, y VisaNet Perú la envía al switch central ATM del Banco de la Nación con el MAC calculado. El Banco de la Nación comprueba los datos de la transacción y envía la respuesta a través de la nube VisaNet Perú, que le responderá al Banco Adquirente y finalmente al cajero automático, con la respuesta al cliente.

- Transacción internacional: cuando un cliente del Banco de la Nación con tarjeta Multired Global Débito, realiza una transacción en un cajero Visa de otro país. El PIN Block generado bajo la TPK, llega al banco y es identificada como transacción doméstica. El Banco envía el PIN Block a la nube Visa, encriptado bajo su IWK, y VisaNet Perú la envía al switch central ATM del Banco de la Nación encriptado bajo la AWK. El Banco de la Nación comprueba los datos de la transacción y envía la respuesta a

través de la nube Visa, que le responderá al Banco Adquirente y finalmente al cajero automático, con la respuesta al cliente.

f. Ambiente de Pruebas

- Conocido también como VTS (Visa Transaction System) simula transacciones con la nube Visa, por lo cual necesita la generación de llaves IWK y AWK de prueba, distintas a las que se encuentran en el ambiente de producción.

g. Coprocesador Criptográfico

- Es una tarjeta con funciones criptográficas que viene instalada en el Computador Central z890, que actualmente es usada de manera paralela a los equipos HSM. Cuenta con los mismos valores de llaves criptográficas CVV, PVV, ZMK y MAC.
- Los canales de atención validados por el coprocesador criptográfico son:
  - Canal Internet: para lo cual cuenta con una llave de transporte TMK, para encriptar toda la información enviada desde la página de Internet hasta el servidor de Internet. Luego, se cuenta con una llave de PIN PVK, para mantener protegido al PIN de internet de 6 dígitos (no es el mismo PIN de 4 dígitos usados para el canal ATM), cuando viaja entre el servidor de internet y el computador central.

  - Canal de ventanillas: La información capturada en los POS de las ventanillas de las agencias del Banco de la Nación es validada en el coprocesador criptográfico. Para ello los POS, al igual que los ATM, cuentan con una llave maestra y una llave de trabajo. La llave maestra es instalada por la Sección Instalación y Configuración. Esta llave maestra es conocida por todo el personal de dicha sección y es única por terminal. La llave de trabajo se encuentra en un archivo que se guarda en los terminales de trabajo del personal de ventanillas.

- Canal telefónico: En el canal telefónico se pueden realizar consulta de saldos y bloqueo de tarjeta. Para ello se debe ingresar el número de DNI o de tarjeta, y el PIN de 4 dígitos. Esta información es protegida con una llave de trabajo generada y almacenada en el coprocesador criptográfico.

- El coprocesador criptográfico no permite a los custodios y/o a la División Seguridad de Información, verificar si los valores ingresados de los componentes o llaves criptográficas han sido ingresados de manera correcta.
- Tampoco permite ver el valor actual de las llaves criptográficas almacenadas en dicha tarjeta.
- La aplicación que se comunica con el coprocesador criptográfico fue desarrollada in-house, y maneja las funciones de encripción y desencripción a través de software.
- Las llaves criptográficas del coprocesador criptográfico se almacenan en archivos, accesibles por personal con acceso al computador central.

3.3 Host Security Module HSM 8000

3.3.1 Seguridad Física

Los comandos de los equipos HSM son activados de acuerdo al acceso físico que se tenga a dichos equipos en un determinado momento. El acceso físico a dichos equipos se realizará a través de dos parámetros:

a. Llaves físicas: los equipos HSM cuentan con dos llaves físicas, las cuales determinan los comandos que pueden ser utilizados. La posición de las llaves físicas determinan un **estado**, como se muestra en la tabla a continuación:

State	Left hand lock	Right hand lock
Normal (online)	Locked (activated)	Locked (activated)
Offline	Locked	Unlocked
Offline	Unlocked	Locked
Secure	Unlocked	Unlocked

Tabla 3.3. Estados posibles del HSM 8000 según llaves físicas [Thales04]

b. Tarjeta o clave autorizadora: de manera paralela, las funciones de los HSM pueden ser configuradas utilizando una clave autorizadora, ingresada bajo control dual. Esta clave puede ser reemplazada por el uso de SmartCards, que pertenecen a los dos primeros custodios de la LMK.

3.4 Organización del Banco de la Nación [BN08]

El Banco de la Nación es una empresa de derecho público, integrante del Sector Economía y Finanzas, que opera con autonomía económica, financiera y administrativa. El Banco tiene patrimonio propio y duración indeterminada.

El Banco se rige por su Estatuto, por la Ley de la Actividad Empresarial del Estado y supletoriamente por la Ley General de Instituciones Bancarias, Financieras y de Seguros.

Es objeto del Banco administrar por delegación las subcuentas del Tesoro Público y proporcionar al Gobierno Central los servicios bancarios para la administración de los fondos públicos.

El Banco de la Nación, para la implementación de las tarjetas Multired Global Débito, se ha organizado y asignado ciertas responsabilidades a las diferentes áreas. En la figura 3.8 se puede apreciar el organigrama del Banco de la Nación, de la cual explicaremos las responsabilidades asignadas:

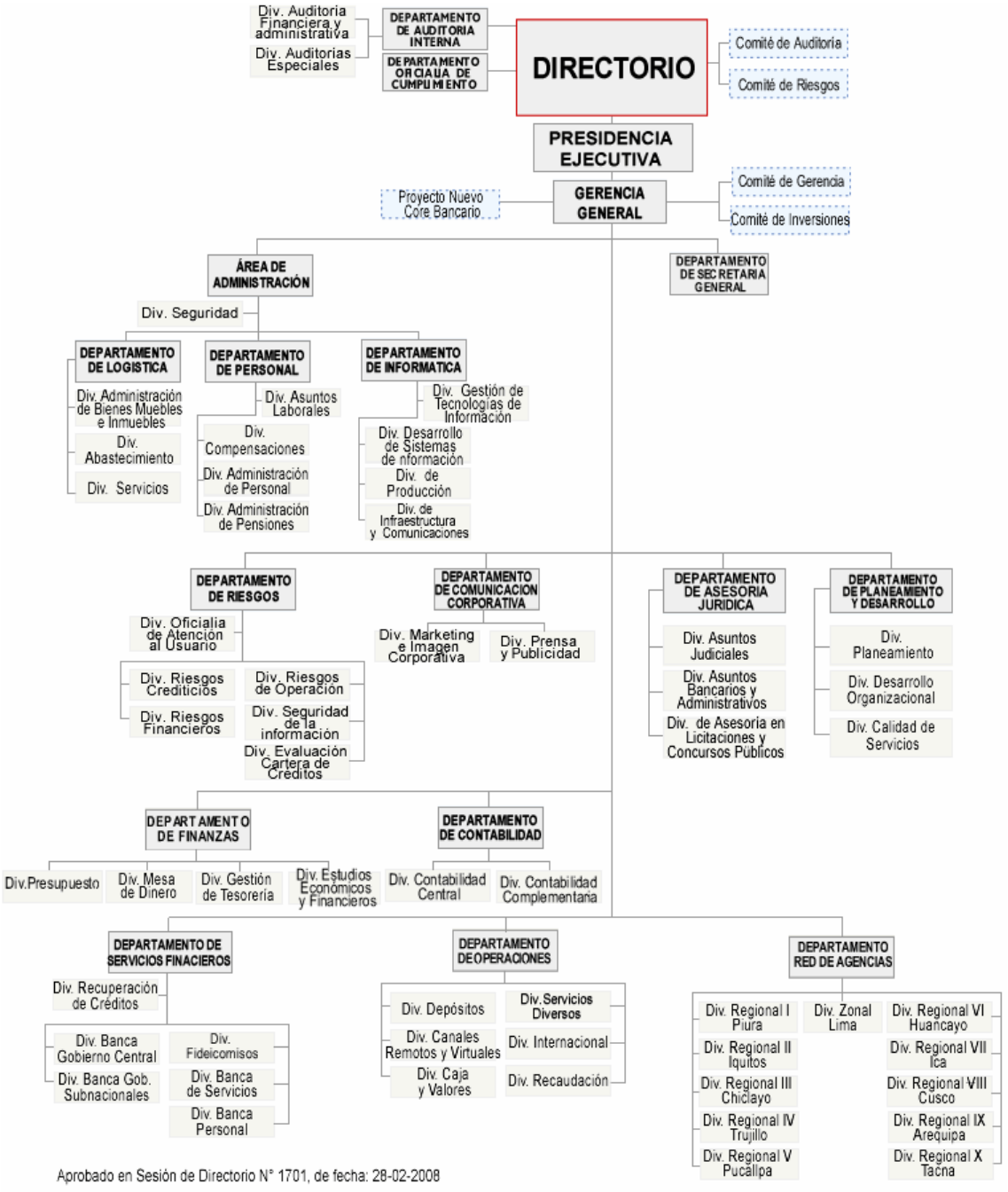


Figura 3.9. Organigrama del Banco de la Nación [BN08]

3.4.1 División Seguridad de Información

- Creada en el año 2004 para el cumplimiento de lo estipulado por la SBS en la Resolución SBS N° 006-2002 Reglamento para la Administración de Riesgos de Operación, bajo el mando directo de la Gerencia General, ahora pertenece a la Gerencia del Departamento de Riesgos.

- Misión: Garantizar un adecuado nivel de seguridad en la administración de la información, brindando las condiciones necesarias para una apropiada administración del acceso y uso de dicha información considerando todos los medios utilizados.
- Su función principal es elaborar y proponer a la Gerencia General y Directorio las políticas de seguridad de información, e implementar las medidas o controles necesarios en la empresa para lograr su cumplimiento.
- Define los controles de seguridad de información para las llaves criptográficas.
- Administra el acceso y uso de las llaves criptográficas y a los equipos HSM.
- Configura los equipos HSM, Switch Central de ATMs, Coprocesador Criptográfico y Tarjetas inteligentes.
- Solicita y autoriza el acceso a las llaves criptográficas, de acuerdo a la situación que se presente.
- Convoca a los custodios de los componentes de claves criptográficas de acuerdo a la situación que se presente.
- Administra el acceso a los aplicativos criptográficos del Banco de la Nación.
- Envía los componentes de TMK a ser instalados en los cajeros automáticos, a los diferentes custodios.

3.4.2 Sección Procesamiento Central

- Pertenece al Departamento de Informática, División de Producción.
- Custodia el Centro de Cómputo Principal, donde se encuentra el HSM 1.
- Autoriza y hace seguimiento del acceso al equipo HSM 1, de acuerdo a la solicitud del jefe de la División Seguridad de Información.
- Monitorea el estado del HSM 1.

3.4.3 Administrador de Agencia (Oficina de Respaldo)

- Pertenece al Departamento de Red de Agencias, División Zonal Lima.

- Custodia el Centro de Cómputo de Respaldo, donde se encuentra el HSM 2.
- Autoriza y hace seguimiento del acceso al equipo HSM 2, de acuerdo a la solicitud del jefe de la División Seguridad de Información.
- Monitorea el estado del HSM 2.

3.4.4 Administradores de Agencias de Provincias

- Pertenecientes a las diferentes zonas de atención del Banco de la Nación en provincias, Departamento de Red de Agencias.
- Instalan el primer componente de la llave TMK en los cajeros automáticos de provincias.
- Verifican el funcionamiento adecuado de los cajeros automáticos.
- Destruyen los componentes de llaves criptográficas una vez ingresados.

3.4.5 Jefes de Operaciones de Provincias

- Pertenecientes a las diferentes zonas de atención del Banco de la Nación en provincias, Departamento de Red de Agencias.
- Instalan el segundo componente de la llave TMK en los cajeros automáticos de provincias.
- Destruyen los componentes de llaves criptográficas una vez ingresados.

3.4.6 Sección Instalaciones y Configuraciones

- Pertenece al Departamento de Informática, División de Infraestructura y Comunicaciones.
- Instala la llave maestra y de trabajo en los POS de las agencias y estaciones de trabajo (ventanillas) respectivamente.
- Instala el primer componente de la llave TMK en los cajeros automáticos de Lima.

3.4.7 Sección Canales Virtuales

- Genera el primer componente de la TMK para los cajeros automáticos.

3.4.8 Sección Canales Remotos

- Genera el segundo componente de la TMK para los cajeros automáticos.
- Instala el segundo componentes de la llave TMK en los cajeros automáticos de Lima.

3.4.9 Gerentes de Departamento

- Son los custodios de las llaves criptográficas LMK, ZMK, MAC, CVK Y PVK.
- Los custodios de llaves maestras y de encripción de llaves son definidos por la institución desde los gerentes de departamento hasta los jefes de división, debido a que el Banco de la Nación define sus puestos como 'de confianza' por lo cual, su responsabilidad con la empresa es mayor.
- Los custodios de llaves de trabajo son definidos por la División Seguridad de Información, de acuerdo a los procedimientos y operatividad interna relacionados a la instalación y mantenimiento de cajeros automáticos.

3.4.10 Departamento de Planeamiento y Desarrollo

- Proponer, validar, aprobar y difundir la normativa interna del Banco de la Nación.

3.4.11 Gerencia General

- Aprobar la normativa interna del Banco de la Nación.
- Nombrar al personal de confianza del Banco de la Nación.

- Reemplazar y/o asumir las funciones de la División Seguridad de Información cuando por algún motivo ésta no pueda realizarlas.

3.5 Estándar EMV

3.5.1 Autenticación Offline Estática de Datos [Visa06B]

- Esta autenticación es llevada a cabo por el terminal usando un esquema de firma digital basado en técnicas de Llaves Públicas.
- Este mecanismo confirma la legitimidad de datos estáticos críticos residentes en la tarjeta chip.
- Requiere la existencia de una Autoridad Certificadora, que es una Entidad altamente segura, que "firma" las Llaves Públicas del Emisor.
- Cada terminal que se ajuste a esta especificación contendrá las Llaves Públicas de la Autoridad Certificadora respectiva para cada aplicación reconocida por el terminal.
- Esta especificación permite que múltiples identificadores de aplicaciones compartan el mismo conjunto de Llaves Públicas de la Autoridad Certificadora.
- La tarjeta le provee al terminal:
  - El Certificado de Llaves Públicas del Emisor (La Llave Pública del Emisor certificada por la Autoridad Certificadora).
  - La aplicación de datos estáticos firmada SSAD, firmada por el Emisor.

Datos requeridos en el ICC para la Autenticación Offline Estática de Datos [Visa06B]

- El índice de la Llave Pública de la Autoridad Certificadora contiene un número binario que indica cuál de las aplicaciones de las Llaves Públicas de las Autoridades Certificadoras y sus algoritmos asociados que residen en el terminal, va a ser usada con esta tarjeta de circuito integrado.

- El Certificado de la Llave Pública del Emisor es suministrado por la Autoridad Certificadora respectiva al Emisor de la tarjeta.
- Cuando el terminal verifica este dato, autentica la Llave Pública del Emisor.
- La aplicación firmada de datos estáticos es generada por el Emisor usando la Llave Privada que corresponde a la Llave Pública autenticada en el Certificado de Llaves Públicas del Emisor.

3.5.2 Autenticación Offline Dinámica de Datos [Visa06B]

- Esta autenticación es llevada a cabo por el terminal usando un esquema de firma digital basado en técnicas de Llaves Públicas.
- Este mecanismo autentica el ICC y confirma la legitimidad de datos residentes y generados por el ICC y datos recibidos del terminal.
- Requiere la existencia de una Autoridad Certificadora, que es una Entidad altamente segura que "firma" las Llaves Públicas del Emisor.
- Cada terminal que se ajuste a esta especificación contendrá las Llaves Públicas de la Autoridad Certificadora apropiada para cada aplicación reconocida por el terminal.
- Esta especificación permite que Múltiples Identificadores de Aplicaciones compartan el mismo conjunto de Llaves Públicas de la Autoridad Certificadora.
- La tarjeta le provee al Terminal:
  - El Certificado de Llaves Públicas del Emisor (La Llave Pública del Emisor certificada por la Autoridad Certificadora).
  - El Certificado de Llaves Públicas del ICC (Llave Pública del IC y la aplicación de datos estáticos firmados por el Emisor).
  - Datos dinámicos de la tarjeta y el terminal firmados por la Tarjeta.
- El terminal:
  - Usa la Llave Pública de la Autoridad Certificadora para verificar que la Llave Pública del Emisor fue certificada por la Autoridad Certificadora.

- Utiliza la Llave Pública del Emisor para verificar que la Llave Pública del IC de la Tarjeta y la Aplicación de Datos Estáticos fue certificada por el Emisor.
- Emplea la Llave Pública del IC de la tarjeta para verificar que los datos fueron firmados por la tarjeta.

Datos requeridos en el ICC para la Autenticación Offline Dinámica de Datos

- El índice de la Llave Pública de la Autoridad Certificadora contiene un número binario que indica cuál de las aplicaciones de las Llaves Públicas de las Autoridades Certificadoras y sus algoritmos asociados que residen en el terminal va a ser usada con esta tarjeta de circuito integrado.
- El Certificado de la Llave Pública del Emisor es suministrado por la Autoridad Certificadora respectiva al Emisor de la tarjeta.
- Cuando el terminal verifica este dato, autentica la Llave Pública del Emisor.
- El Certificado de la Llave Pública de la tarjeta de circuito integrado es provisto por el Emisor a la tarjeta de circuito integrado.
- Cuando el terminal verifica este dato, autentica la Llave Pública del ICC.
- Para apoyar esta autenticación el ICC tendrá su propio par de Llaves Públicas.
- Estas consisten de la Llave Privada para la Firma y la correspondiente Llave Pública para la verificación.
- La Llave Pública del ICC estará almacenada en el ICC en un Certificado de Llaves Públicas.
- Un esquema de tres capas de certificación de Llaves Públicas es empleado.
- La Llave Pública del ICC es certificada por su Emisor y la Autoridad Certificadora verifica la Llave Pública del Emisor.
- Esto implica que para la verificación de la Firma de un ICC, el terminal primero necesita verificar dos certificados para poder obtener y autenticar la Llave Pública del ICC.

- Por último la Llave Pública del ICC es entonces empleada para verificar la Firma Dinámica del ICC.

3.5.3 Cifrado del PIN offline [Visa06B]

- Para la verificación del PIN offline el cifrado del PIN es llevado a cabo por el terminal usando criptografía asimétrica.
- Este mecanismo asegura la transferencia segura del PIN desde el PIN pad evidente a las alteraciones hasta el ICC.
- El ICC tendría un par de llaves asociado al cifrado del PIN.
- La llave pública es usada por el PIN pad o el componente seguro del terminal para cifrar el PIN.
- La llave privada es usada por el ICC para descifrar el PIN cifrado para su verificación.
- Puede usarse un componente seguro del terminal en lugar de un PIN pad para el cifrado del PIN.
- Entonces el transporte del PIN desde el PIN pad hasta el componente seguro debe asegurar su secreto.
- Cuando el terminal permite la verificación del PIN offline, el dispositivo de entrefase (IFD) y el PIN pad pueden estar integrados en un mismo dispositivo que sea evidente a las alteraciones.
- O pueden ser dos dispositivos separados evidentes ambos a las alteraciones.

Cifrado del PIN

- Si el dispositivo de entrefase y el PIN pad están integrados y el PIN offline se transmite a la tarjeta en claro, entonces el PIN Pad no cifra el PIN offline cuando el PIN en claro es enviado directamente del PIN pad al IFD
- Si el dispositivo de entrefase y el PIN pad están integrados y el PIN offline se transmite a la tarjeta en claro, pero el PIN offline en claro no es enviado

directamente desde el PIN pad integrado al IFD, entonces el PIN pad debe cifrar el PIN offline para su transmisión al dispositivo de entrefase

- En este caso el dispositivo de entrefase descifrará el PIN offline para su transmisión en claro a la tarjeta
- Si el dispositivo de entrefase y el PIN pad no están integrados y el PIN offline se transmite a la tarjeta en claro, entonces el PIN Pad cifrará el PIN offline para su transmisión al dispositivo de entrefase
- Posteriormente el dispositivo de entrefase descifrará el PIN offline para su transmisión en claro a la tarjeta
- Si el PIN offline se transmite a la tarjeta cifrado, entonces el PIN debe ser cifrado en el mismo PIN pad evidente a las alteraciones o en un componente seguro en la terminal
- En este caso, el PIN pad cifrará el PIN para su transporte seguro entre el PIN pad y el componente seguro

3.5.4 Principios de Administración de llaves y tipos de llaves criptográficas para tarjetas de circuito integrado (Integrated Circuit Card ICC) [EMVCo03]

Diferentes tipos de algoritmos criptográficos soportan las diferentes funciones del estándar EMV. Sin embargo, una incorrecta implementación de dichos algoritmos impactará negativamente en la empresa. Una implementación segura dependerá de que tan bien las llaves criptográficas requeridas por la especificación sean administradas por el emisor. Los siguientes controles son provistos para mantener seguras las llaves criptográficas:

3.5.4.1 Administración de llaves asimétricas (RSA)

La seguridad de las tarjetas chip depende de la protección de las llaves privadas (firma). La falla de la seguridad en las llaves privadas usadas para firmar elementos de datos estáticos arriesga la creación de tarjetas

IC falsificadas. Los riesgos primarios de las llaves privadas incluyen: la fabricación de los módulos RSA y el compromiso de las llaves privadas.

La seguridad de las llaves privadas depende de un número de factores, incluidos:

- La longitud en bits de la llave RSA; por ejemplo: 768, 896,1024, 1152.
- La calidad de los números primos generados por el módulo de las llaves públicas y privadas.
- Los métodos usados para proteger físicamente la llave privada de excesos no autorizados y exposición o compromiso.

a. Longitud de llave y criptoperíodo

La longitud del algoritmo RSA está relacionada exponencialmente a la longitud de la llave. El tamaño de la llave está en bits. EMV ha recomendado el siguiente esquema de tamaño de llaves y criptoperíodos para las llaves RSA:

TAMAÑO DE MÓDULO	EXPONENTE DE LLAVE PÚBLICA	CRIPTOPERÍODOS
768 bits	3 o $2^{16} + 1$	31/12/2002
896bits	3 o $2^{16} + 1$	31/12/2004
1024bits	3 o $2^{16} + 1$	31/12/2008
1152bits	3 o $2^{16} + 1$	31/12/2010

Tabla 3.4. Tamaño de llaves EMV y criptoperiodos [EMVCo03]

En el caso del que el emisor detecte que su llave privada correspondiente a su certificado de llave pública del emisor ha sido comprometida, es recomendable que el par de la llave comprometida sea reemplazada y re-emitida para tarjetas con certificado de llave

pública creadas por la llave comprometida para mitigar el riesgo de fraude.

b. Generación de llaves RSA

Cuando se genera un par de llaves pública/privada RSA, es recomendable que el proceso sea completado en la memoria protegida de un equipo físicamente seguro. Ya que un equipo debe contener un generador de números aleatorios o pseudoaleatorios, configura rutinas de chequeo y soporta mecanismos contra alteración.

- La llave privada RSA puede permanecer efímera al equipo físicamente seguro.
- La generación de llaves debe utilizar un proceso aleatorio o pseudoaleatorio, tal que no sea posible predecir ninguna llave o determinar que ciertas llaves son más probables que otras.
- El equipo físicamente seguro usado para crear el par de llaves RSA y asegurar la llave privada, debería satisfacer el set de requerimientos de seguridad descritos en "Equipos Criptográficamente Seguros".
- Un computador personal u otro equipo inseguro y no confiable, no debería ser usado nunca para generar un par de llaves Pública/Privada RSA.
- Los números generados para un proceso de generación de llaves RSA deben ser generados y escogidos aleatoriamente.

c. Uso de llaves

El estándar EMV requiere que las llaves criptográficas sean usadas sólo para el propósito para el cual fueron creadas.

- El par de llaves pública/privada del emisor debe ser única por cada esquema.

- Las llaves del esquema EMV pueden ser usadas sólo en un certificado de llaves públicas por esquema.
- La Autoridad de Registro (o equivalente) responsable de la firma de las llaves públicas del emisor debe asegurar que la llave debe ser firmada es una llave auténtica recibida de una emisor genuino.
- Los emisores deben asegurar que cualquier llave pública que ellos reciban sean que ellos reciban sean auténticas.
- Si una tarjeta IC es usada para generar una firma usando RSA, éste debería verificar la prioridad del certificado/firma para proteger contra ataques.

d. Transporte y almacenamiento de llaves

Para proteger la integridad de un par de llaves pública/privada, es importante que:

- Las llaves públicas sean aseguradas y transportadas de manera que garanticen su integridad. Es recomendable que las llaves públicas sean transportadas dentro de una estructura de datos tal como un certificado, o con un Código de Autenticación de Mensaje (MAC) para la llave pública y datos asociados, usando un algoritmo definido por la ISO 9807 Banking and related financial services - Requirements for message authentication, y una llave usada sólo para ese propósito. También es recomendable que las técnicas de control dual sean usadas para asegurar que el recipiente de la llave pública tiene la habilidad de verificar su origen e integridad; por ejemplo separar y transferir independiente de un valor de chequeo en la llave pública.
- Las llaves privadas deben ser aseguradas y transportadas de manera que garantice su integridad y confidencialidad. Los mecanismos de transporte incluyen:
  - Un equipo criptográfico seguro.

- Cifrado usando un algoritmo simétrico de por lo menos la misma fortaleza criptográfica equivalente a la llave privada de la llave protegida inicialmente.
- Como fragmentos, asegurados en tokens y cifrados usando un algoritmo simétrico.

- Las estrategias de renovación del negocio requerirán la generación y aseguramiento de copias de llaves privada/pública. Estas llaves son necesarias en caso se produzca un evento catastrófico con las llaves del sistema. Las copias de respaldo de las llaves del sistema son aseguradas usando los mismos principios descritos para las llaves originales.

e. Destrucción de llaves

- Los datos de llaves obsoletas deberían ser destruidas usando métodos que sean apropiados para el medio que contiene el material de las llaves. Para una llave almacenada en una tarjeta chip, un método simple es hacer un orificio a través del chip después de los métodos de borrado de chip disponibles.
- Las llaves almacenadas en un equipo criptográfico seguro deberían ser borradas por los mecanismos de seguridad del equipo.
- Una tercera parte independiente, como un auditor interno, debería ser testigo de la destrucción del material de las llaves, documentando el proceso. La documentación debería ser almacenada por un período consistente con las políticas de almacenamiento de documentación del emisor.
- El principio básico para la destrucción de llaves es que una llave puede ser destruida cuando se sabe que ésta ya no es requerida. Las llaves asimétricas del emisor deberían ser retenidas como sigue:
  - Llaves de firma RSA del emisor (privadas): destruir cuando la fecha de expiración de la llave ha llegado.

- Llaves de verificación RSA del emisor (públicas): retenidas hasta que no se espere o presente ninguna disputa de ninguna tarjeta con un certificado con esa llave.
- Todo esquema de llaves firmado con versiones de llaves públicas RSA - retenidas hasta que no se espere o presente ninguna disputa de ninguna tarjeta con un certificado con esa llave.

f. Equipo de aceptación de tarjeta

- Debe tener la capacidad de habilitar la lectura, actualización y mantenimiento seguro de las llaves públicas.
- Debe estar habilitado para seleccionar la llave y el algoritmo correspondiente en conjunción con el identificador del proveedor de la aplicación registrada de la aplicación seleccionada.

3.5.4.2 Administración de Llaves Simétricas

Las llaves DES en la especificación EMV son usadas para funciones de transacciones específicas. Las llaves DES son derivadas de una Llave Maestra de Derivación (Master Derivation Key) en el momento de la personalización. Las llaves resultantes para tarjetas son únicas.

Las llaves Maestras DES de Emisor incluyen:

- Issuer Master Derivation Key (IDK_{AC}) - Llave Maestra de Derivación de Emisor: usada para derivar las llaves de tarjetas que son empleadas para generar MACs conocidas como Criptogramas de Aplicación (Application Cryptograms AC).
- Issuer Secure Messaging Master Keys (IMK_{SMK} IMK_{SMI}) – Llaves Maestras de Mensajería de Seguridad de Emisor: usada para derivar las llaves de tarjetas en la mensajería de seguridad de procesos de emisión de certeza entre una tarjeta y un sistema de autorización;

por ejemplo: bloqueo de tarjeta, bloqueo/desbloqueo de aplicación, datos específicos de actualización de tarjeta, y cambios de PIN.

Cabe resaltar que un emisor puede usar varias IMK para el mismo propósito.

a. Longitud de llaves y criptoperíodos

- Todas las llaves maestras DES EMV tienen 16 bytes o 128-bits de longitud
- Las llaves deben ser reemplazadas cuando su compromiso es conocido o sospechado.

b. Generación de llaves

Los siguientes principios son usados por emisores para minimizar la oportunidad de compromiso de los datos de las llaves durante su creación:

- Cuando las llaves DES con creadas deben ser generadas dentro de un equipo físicamente seguro, protegido por mecanismos de respuesta a intrusiones, o por personal autorizado en forma de un componente. El equipo debe contener un generador de números aleatorios o pseudoaleatorios.
- En ningún momento una llave no protegida podrá existir fuera de una memoria protegida de un equipo físicamente seguro. El texto en claro nunca debe ser sacado del equipo físicamente seguro en formas que no sean en un criptograma o en la forma de dos o más componentes.
- Cuando las llaves secretas son generadas por personal autorizado a través de un proceso de combinación de componentes, cada parte debe ser requerida para generar un componente que es tan largo como la llave a ser generada. El proceso de combinación de llaves debe darse a lugar dentro de un equipo físicamente seguro. Además, el método de combinar componentes deberá ser tal que el

conocimiento de un componente no lleve al conocimiento del valor de la llave completa. Los componentes de las llaves deberán ser custodiados por personal de la empresa emisora.

- Los dígitos de chequeo deben ser calculados a partir de componentes de llaves de 16 bytes o de la llave completa.
- Un computador personal o equipos inseguros similares no deben ser usados para generar material de llaves.
- Si una llave criptográfica es encontrada que existe fuera de un equipo físicamente seguro o los componentes de la llave criptográfica son conocidas o se sospecha que han estado bajo el control de un solo individuo, la llave debe ser considerada de haber sido comprometida y debe ser reemplazada por una nueva llave.

c. Uso de llaves

El uso de llaves ocurre cuando una llave es empleado para un propósito criptográfico. Una llave debe ser usada sólo para el propósito criptográfico para el cual es creada y para ningún otro propósito.

d. Transporte y almacenamiento de llaves

Puede ser necesario transportar y/o almacenar llaves DES. Cuando las llaves DES son transportadas o almacenadas, las siguientes medidas deberían limitar el potencial de compromiso de la data:

- Llaves DES en texto claro pueden ser seguramente transferidas para la protección de un token seguro o una tarjeta inteligente tanto para el transporte como para el almacenamiento.
- Las llaves DES pueden ser sólo transportadas o almacenadas fuera de una memoria protegida de un token seguro o una tarjeta inteligente en una de las siguientes formas:
  - En la forma de dos o más componentes usando los principios de control dual y conocimiento compartido.

- Como un criptograma, creado para transportar o almacenar la llave que ha sido establecida seguramente por las partes.

e. Destrucción de llaves

- Los datos obsoletos de llaves deben ser destruidos usando métodos que son apropiados para contener material de llaves. Para una llave almacenada en una tarjeta chip, un método simple es hacer un orificio a través del chip después de los métodos de borrado de chip disponibles.
- Las llaves almacenadas en un equipo criptográfico seguro deberían ser borradas por los mecanismos de seguridad del equipo.
- Una tercera parte independiente, como un auditor interno, debería ser testigo de la destrucción del material de las llaves, documentando el proceso. La documentación debería ser almacenada por un período consistente con las políticas de almacenamiento de documentación del emisor.
- El principio básico para la destrucción de llaves es que una llave puede ser destruida cuando se sabe que ésta ya no es requerida. Las llaves simétricas del emisor deberían ser retenidas hasta que no se espere o presente ninguna disputa de ningún criptograma de aplicación creado por alguna tarjeta que contiene llaves diversificadas de estas llaves.

f. Respaldo y archivo de llaves

Puede ser necesario recuperar llaves usadas para la personalización de tarjetas. Luego, será necesario que ciertas llaves criptográficas sean seguramente respaldadas o archivadas. Cuando el respaldo de las llaves maestras críticas usadas en la personalización de las tarjetas, los siguientes pasos son recomendados:

- Cuando una llave criptográfica no esté encriptada bajo otra llave de igual tamaño, ésta debe ser mantenida como dos o más componentes

asegurados usando los principios de control dual y conocimiento compartido.

- Cuando la llave criptográfica no es asegurada como dos o más componentes usando principios de control dual y conocimiento compartido, ésta debe ser mantenida como un criptograma bajo una llave de almacenamiento única de igual tamaño que es mantenida en un token seguro.
- Los procedimientos de auditoría deberían ser implementados para asegurar que las prácticas mencionadas son implementadas.

g. Equipo de aceptación de tarjeta

Configurado para el cifrado del PIN, debe soportar técnicas de administración de llaves para algoritmos de llaves simétricas como los descritos en ISO 11568-2. Las llaves secretas de un algoritmo de llaves simétricas deben ser protegidas de revelación, y deben ser únicas.

3.5.4.3 Generación de Llaves – Guía General

Toda generación de llaves debería tomar lugar de acuerdo al proceso definido. Este proceso debe ser definido en adelante y todos los roles necesarios presentados en el momento apropiado. El proceso exacto usado depende del sistema con el que se cuente. El ambiente en el cual la generación de la llave toma lugar debe ser seguro. Éste debe ser apropiado para los métodos y equipamiento que son usados y la configuración del equipamiento no debe dejarlo expuesto a ataques como escucha electromagnética.

Para cada tipo de llave, un procedimiento debería ser creado de tal manera que permita definir detalles de la localización, métodos, equipos y roles de custodios necesitados por sesión. El procedimiento debería ser explícito y fácil de seguir para todos los roles, y que soporte la idea

de que para el ingreso de los fragmentos de llaves de los custodios no será necesario usualmente un conocimiento profundo del proceso a ser usado, y la configuración de dichas llaves no sea realizado de manera frecuente.

El procedimiento debería establecer quién está autorizado para iniciar su ejecución. Éste debería definir cómo el sistema de generación de llaves es establecida y qué acciones son necesarias luego de su uso para su almacenamiento seguro. Éste debería establecer cómo los fragmentos de llaves serán almacenadas y por quién.

El procedimiento debería también definir como las copias de las llaves deben ser generadas y cómo ellas deben ser protegidas. Se debe notar que al menos dos copias de la mayoría de las llaves serán necesarias – una para el uso en producción y una para su almacenamiento en el sitio de respaldo. La copia de respaldo debería estar protegida al menos tan bien como la copia de producción.

El objetivo es crear un procedimiento que sea ampliamente auto-documentable tal que un auditor pueda usar una copia del procedimiento, autorizaciones originales y registros de auditoría firmados por los participantes –luego del evento– para concluir que las llaves han sido seguramente generadas, almacenadas y usadas.

3.5.4.4 Custodia de Llaves – Prácticas y Responsabilidades

a. Reunión de personal de administración de llaves

- El personal responsable de administrar las llaves de encripción y componentes de llaves, tokens seguros y otros equipos de material de llaves deben ser designados por terceras partes.

- Cuando se designa personal para ser responsables del control de la custodia de datos de llaves o tokens seguros, controles suficientes deben ser implementados para asegurar que ningún individuo o individuo no autorizado puede obtener acceso a los datos inmersos en una llave criptográfica o en un token seguro.
- Los custodios de llaves deberían ser empleados confiables, no consultores o empleados temporales.
- Para asegurar la continuidad de los servicios, personal alterno puede ser también ser identificado como "respaldos" para los custodios principales. El criterio usado para seleccionar los custodios de respaldo debe ser el mismo que los usados para seleccionar los custodios principales.

b. Funciones del personal de administración de llaves

Las responsabilidades de custodia de llaves son importantes y una parte fundamental del protocolo de seguridad de un emisor. Los datos de llaves que serán administrados por estas personas representan las llaves más importantes en las aplicaciones criptográficas para un programa de emisión de tarjetas. Cada emisor debe revisar sus procedimientos de administración de llaves y los roles de cada custodio.

- Las responsabilidades del personal de administración de llaves incluyen el control del material de llaves, verificación del material y su almacenamiento seguro.
- Los custodios de llaves o sus respaldos son responsables de:
  - Recepción y almacenamiento seguro de componentes de llaves y/o tokens seguros.
  - Mantenimiento de registros o acceso a logs de grabación y uso de datos de llaves, incluyendo tiempo de acceso, fecha, propósito y retorno para almacenamiento seguro.
  - Evidencia de destrucción de obsolescencia/antigüedad de componentes de llaves.

- Ingreso de datos de llaves dentro de un módulo criptográfico seguro como se requiera cada cierto tiempo.
- Dirección y verificación de la destrucción de material de llaves obsoletas, como indique el propietario de los datos.

➢ Los custodios de los datos de la llave donde es originada inicialmente son responsables de la seguridad y resguardo de los datos que son designados a su contraparte de la entidad receptora. Esta responsabilidad incluye la verificación de la recepción de los datos.

3.5.4.5 Equipos Criptográficamente Seguros (Secure Cryptographic Devices SCD)

Los SCD son usados en los estándares ISO para describir un arreglo ordenado de equipamiento usado para proveer cierta protección para operaciones criptográficas. Al final del arreglo de SCDs se encuentran los módulos hardware de seguridad (HSMs) conectados a procesadores Host, equipos de personalización y sistemas de autorización. En el lado opuesto del espectro están los tokens de seguridad y Tarjetas de Circuito Integrado (ICC).

El material contenido aquí será usado para realzar el conocimiento del lector y el entendimiento de los atributos de seguridad requeridos por los esquemas de pago como parte de sus prácticas de administración de riesgos. Los esquemas internacionales de tarjetas deben ser consultados respecto a sus requerimientos individuales para SCDs, particularmente cuando el SCD s usado en un ICC.

a. Requerimientos de resistencia a alteración

La resistencia a alteración puede ser separada en dos dominios: físico y lógico.

- **Atributos de seguridad física:** la seguridad física consiste en los siguientes atributos:
  - Protección contra penetración incluyendo el borrado de data sensible.
  - Protección contra modificaciones no autorizadas que pudieran resultar en revelación de información sensible.
  - Protección para prevenir el monitoreo de emisiones electromagnéticas resultado de la operación del equipo.

- **Atributos de seguridad lógica:** las características de seguridad lógica consiste en los siguientes atributos:
  - Verificaciones de genuinidad.
  - Diseño de la función de configuración del equipo que asegure que ninguna función individual o combinación de funciones de los equipos resultará en revelación de información sensible.
  - Mecanismos existentes de aseguramiento de segmentación de llaves criptográficas.
  - Las operaciones sensibles de estado requieren control dual.
  - Inclusión de técnicas para la autenticación de descarga de software.

b. Almacenamiento de llaves

- **Hardware vs. Software**

Es común pensar que las llaves comienzan a ser almacenadas en una localización de 'hardware' como en un HSM o una localización de 'software' como en un sistema de computadores host. En realidad, éstos son justamente anotaciones no documentadas para un juego de asunciones sobre cómo una llave puede ser comprometida.

Las llaves son generalmente almacenadas en medios magnéticos como discos, memorias volátiles o memorias de almacenamiento de mayor capacidad tales como las usadas en las tarjetas IC. Las llaves son protegidas de una variedad de ataques físicos tales como resistencia contra intrusión de un HSM o una tarjeta IC y la protección lógica de un sistema operativo en HSMs (o SCDs), tarjetas IC y computadores host.

El almacenamiento de llaves en medios magnéticos debe ser considerado como temporal. El tiempo de vida de un diskette debería ser asumido como no más de par de años.

El almacenamiento en memorias de silicón no volátiles tiene un potencial de vida típica de al menos 10 años.

Sin embargo las llaves son almacenadas, y necesitan protección contra compromiso. Los equipos que almacenan llaves deberían ser aseguradas físicamente –por ejemplo, en un paquete que evidencie alteración. Los equipos que usan llaves deberían verificar su integridad antes de su uso. Esto es especialmente importante para las llaves cifradas almacenadas en una base de datos. Mientras que esto puede no ser posible para leer llaves cifradas, esto podría ser alterado para permitir otras formas de ataque. Cuando una llave almacenada en un equipo seguro como una tarjeta IC es verificada, un dígito de chequeo no criptográfico sería suficiente. Donde sea abierto para alteración como en una base de datos, es cuando se requiere un MAC criptográfico.

- **El uso de consolas PC:**

Una consola PC que provee servicios criptográficos a un host que debería ser visto como una forma de HSM con niveles similares de protección esperada.

Se debe notar que la razón principal para el uso de equipos criptográficamente seguros es proteger las llaves. Si el sistema host que usa el HSM es en sí mismo inseguro, puede ser fácil de atacar y comprometer las funciones del software del sistema, ignorando el HSM.

- **Controles de Acceso**

  Todas las llaves almacenadas fuera de una tarjeta o fuera de un HSM deberían ser accedidas como mínimo bajo control dual.

- **Memoria segura del HSM e IC**

  Un HSM y un IC comparten un número de características y difieren radicalmente en otras. En general, un HSM puede contener por separado los equipos de almacenamiento y procesamiento, y el material de llaves pasará entre buses de hardware internos. Por esta razón es importante que el HSM limpie su memoria cuando se detecta compromiso del mismo. También es importante que el diseño del hardware del HSM direccione la radiación electromagnética. Los HSMs son diseñados en general para ser usados en un ambiente desprotegido. En general la confiabilidad de la resistencia a alteración en la memoria protegida.

3.5.4.6 El Sistema de Autorización

La autorización es un proceso por el cual un emisor, o un representante del emisor, aprueban una transacción de su tarjetahabiente. La

autorización es una respuesta a una solicitud de autorización del comercio o del adquirente.

La solicitud de autorización incluye un criptograma de autorización generado por la tarjeta (Authorization Request Card ARQC) para transacciones que requieren autorización en línea. El emisor valida el ARQC durante el proceso de autenticación en línea de la tarjeta para asegurar que la tarjeta es auténtica y no creada usada datos falsos.

En respuesta al ARQC, el emisor opcionalmente crea un criptograma de respuesta de autorización (Authorization Response Card). Este criptograma es el resultado de encriptar el ARQC y la respuesta de autorización usando una llave de derivación única para la tarjeta. La tarjeta valida el ARPC para asegurar que la respuesta de autorización provenga del emisor. La integridad del proceso de autorización está basada en la protección de la llave de derivación única maestra. Luego, el emisor debería tomar el mismo cuidado en la protección de la confidencialidad de su llave criptográfica cuando es usada en el sistema de autorización del emisor cuando éste sea usado para la personalización de la tarjeta. Luego, los principios de administración de las llaves simétricas descritas anteriormente son recomendadas para asegurar la integridad criptográfica en el proceso de autorización.

3.5.4.7 Seguridad de la Aplicación de la Tarjeta IC

La administración de la seguridad para la aplicación de la tarjeta incluye varios factores:

- La plataforma del IC
- Seguridad de desarrollo de la aplicación
- Seguridad de datos de la aplicación post-emisión
- Seguridad de los comandos ADPU

La plataforma IC debe ser la que ha sido aprobada por el esquema de pago de quien la aplicación basada en EMV está siendo usada. No todas las plataformas IC proveen necesariamente seguridad para proteger los intereses del esquema o del emisor.

La aplicación software debería ser desarrollada en un ambiente controlado. Este ambiente no sólo debería ser físicamente seguro, sino ser administrado usando procedimientos que aseguren la integridad de la aplicación y del código fuente.

Los datos que serán usados para la personalización deberían ser administrados de acuerdo con los datos existentes y las políticas de seguridad de tecnologías de información del emisor. Los datos secretos de la aplicación, incluyendo las llaves criptográficas, PINs y otros datos designados como secretos, deberían ser asegurados, accesibles sólo por personal autorizado.

Los datos secretos de la aplicación no deberían ser accesibles fuera de rutinas especificadas por la aplicación. Consecuentemente, los métodos no documentados de actualización, reseteo o data de incremento deberían ser permitidos.

a. Consideraciones de Seguridad de Implementación

Las técnicas de ingeniería de seguridad de tecnologías de información requieren que los mecanismos de protección sean implementados para asegurar la integridad y seguridad de la aplicación durante su desarrollo e implementación. Decidir cuál de estos mecanismos son relevantes para una implementación particular requiere un entendimiento de los ambientes de desarrollo e implementación. La siguiente es una lista de

las consideraciones más importantes que deberían ser usadas en el desarrollo e implementación de una aplicación basada en EMV.

- Limitar el uso de algoritmos simétricos para proteger contra ataques que puedan comprometer llaves criptográficas.
- Contadores de ingreso de PIN deberían estar siempre actualizados para la comparación del ingreso del PIN del tarjetahabiente con la referencia PIN. Los contadores de intento de PIN deberían ser reseteados a 0 sólo luego de una comparación exitosa o en respuesta a un comando de reseteo de un mensaje de seguridad que ha sido exitosamente verificado.
- Proteger contra la configuración o personalización incorrecta y corrupción de datos deliberada o accidentalmente.
- Usar dígitos de chequeo para proteger contra corrupción deliberada o accidental de datos estáticos.
- Asegurar que la aplicación no sea dejada en un estado inseguro cuando la electricidad es interrumpida o removida.
- Hacer que los contadores de seguridad relacionados estén disponibles para propósitos de diagnóstico.
- Proteger contra ataques basados en análisis de poder en la comparación de campos de datos con el texto plano o desencriptado del PIN Block para la verificación de la encripción del PIN.

3.5.4.8 Detección de Fraude

El emisor debería proactivamente monitorear las transacciones EMV para detectar el posible uso fraudulento de tarjetas y terminales EMV. Algunas áreas de monitoreo incluyen:

- Indicadores en línea: cuando tomar una decisión implica aprobar o declinar una transacción, considerando el uso de indicadores que son enviados en línea en los datos de la aplicación del emisor y otros elementos de datos en línea. Éstos incluyen fallas de autenticación

de datos fuera de línea, fallos del PIN fuera de línea e ingreso de PIN.

- Criptogramas en línea: validar el criptograma para el mensaje de autorización y borrado, para asegurar la validez de la tarjeta.
- Banda magnética de lectura de tarjetas chip en terminales chip: éstos pueden ser un indicador de fraude pero también pero causar problemas con el chip o lector de chip.
- Datos de chip inconsistentes: chequear que los datos recibidos del chip en el mensaje de autorización y borrado es consistente con qué es personalizado o actualizado en la tarjeta.
- Comandos script: asegurar que las transacciones del chip leído no sean recibidas de tarjetas o aplicaciones que fueron previamente bloqueadas usando comandos scripts.

Las siguientes acciones deberían ser tomadas para prevenir fraude y pérdidas de crédito.

- Bloquear la aplicación o la tarjeta cuando la tarjeta es robada.
- Ajustar los límites de velocidad para reflejar la actualización de cambios realizados por el tarjetahabiente.

Capítulo 4: Análisis de Riesgos

En este capítulo se analizarán los riesgos de la actual implementación de la tecnología alrededor de la criptografía del Banco de la Nación, a partir de los cuales se identificarán los controles de seguridad de información, objetivo de este trabajo de investigación.

Los riesgos identificados contarán con una numeración que obedecerá al área del cual se desprenden. Esto permitirá que los controles identifiquen fácilmente el riesgo que está mitigando.

4.1 De la evaluación de riesgos

Una evaluación de riesgos realizada adecuadamente, debe evaluar la probabilidad y el impacto de dichos riesgos, en caso de que éstos se concreten.

La probabilidad nos indica el número de veces que un riesgo puede ocurrir, dada el contexto vigente en el que este riesgo se puede desarrollar. El impacto nos indica la severidad que, de concretarse el riesgo, tendría sobre la empresa.

Según estos conceptos, un riesgo es evaluado y se determina su ***criticidad***. Para ello se establece el siguiente cuadro de Nivel de Criticidad de Riesgos:

Probabilidad / Impacto	Baja	Media	Alta
Bajo	Baja	Media	Media
Medio	Media	Media	Alta
Alto	Alta	Alta	Alta

Tabla 4.1. Nivel de Criticidad de Riesgos

Con la información presentada en el Estado del Arte, se evaluará el nivel de criticidad de los riesgos identificados en la administración de las claves criptográficas del Banco de la Nación, relativas a las operaciones en cajeros automáticos.

4.2 De las Claves Criptográficas electrónicas

4.2.1 Generación

R1.1.1. Los componentes de claves criptográficas podrían ser conocidos por más de un custodio, si éstos se generan a voluntad (no de manera aleatoria), con valores conocidos o escogidos por los custodios respectivos.

Probabilidad: Baja Impacto: Alto Criticidad: Media

R1.1.2. Las claves criptográficas podrían ser fácilmente accesibles y/o conocidos sus valores, si no son generadas en un equipo o software que asegure que la generación de sus componentes es aleatorio.

Probabilidad: Baja Impacto: Alto Criticidad: Media

R1.1.3. Las claves criptográficas podrían ser de conocimiento de personas ajenas, si éstas se generan a partir de valores conocidos por una sola persona.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.1.4 Se paralizan las actividades de muchos o todos los cajeros automáticos, al comprometerse la seguridad de la claves o los componentes de claves criptográficas utilizada en dicho canal.

Probabilidad: Baja Impacto: Media Criticidad: Media

R1.1.5. Los componentes de claves criptográficas son conocidos por personas ajenas, ya que se encuentran almacenados de manera electrónica en texto claro.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.1.6. Las claves criptográficas son conocidas por terceros, ya que se vulnera la confidencialidad de sus componentes.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.1.7. Las claves criptográficas son conocidas por terceros, ya que se encuentran almacenadas electrónicamente en texto claro.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.1.8. Las claves criptográficas son conocidas por terceros, ya que se generan utilizando un algoritmo que no ofrece un nivel de seguridad adecuado.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R1.1.9. Los componentes de claves criptográficas son conocidos por terceros, al ingresarse sus valores en equipos que no están instalados con medidas de seguridad de acceso adecuadas.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.1.10 Las claves y componentes de claves criptográficas son conocidos por terceros, al almacenarse electrónicamente en equipos que no identifican o notifican sobre intrusiones y/o manipulación.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R1.1.11. No es posible identificar ante un error, la clave o componente de clave criptográfica cuyo valor es incorrecto o ha sido alterado en el proceso de generación de claves.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R1.1.12. Se accede fácilmente a las funciones de encripción y eliminación de claves criptográficas, por no contar con controles de acceso lógico a dichas funciones.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

4.2.2 Segregación

R1.2.1. La información de más de un canal de atención se compromete, al compartir la misma clave criptográfica entre sí y verse comprometida la seguridad de dicha clave o de sus componentes.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.2.2. La información de más de un canal de atención se compromete, al compartir uno o más componentes de clave criptográfica entre sí y verse comprometida la seguridad de dicho(s) componente(s).

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.2.3. La información privada de clientes o del banco se compromete, al utilizar en el ambiente de producción una o más claves o componentes de claves criptográficas de los ambientes de desarrollo y/o prueba.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

4.2.3 Reemplazo

R1.3.1. La información privada de clientes o del Banco se compromete, al no destruir de manera segura las claves o componentes de claves criptográficas que ya no son usados.

Probabilidad: Baja Impacto: Media Criticidad: Media

R1.3.2. La información privada de clientes o del Banco se compromete, al utilizar componentes de claves criptográficas de los cuales no se tiene seguridad de su confidencialidad.

Probabilidad: Baja Impacto: Alta Criticidad: Alta

R1.3.3. La información privada de clientes o del Banco se compromete, al utilizar equipos no seguros para el cifrado de dicha información.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.3.4. La información privada de clientes o del Banco se compromete, al utilizar claves y/o componentes de claves criptográficas derivadas de otras claves cuya seguridad ha sido vulnerada.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

4.2.4 Transporte

R1.4.1. Se compromete la seguridad de claves criptográficas privadas, al viajar por la red de comunicaciones en texto plano.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.4.2. Se compromete la seguridad de claves criptográficas privadas, al viajar por la red de comunicaciones encriptadas bajo claves que no fueron creadas de manera exclusiva para el transporte de información electrónica.

Probabilidad: Baja Impacto: Medio Criticidad: Media

R1.4.3. Los componentes de claves criptográficas son conocidos por personas ajenas ya que éstos se envían en texto claro entre el Banco de la Nación y Visa Internacional.

Probabilidad: Baja Impacto: Alto Criticidad: Media

4.2.5 Destrucción

R1.5.1. No es posible acceder nuevamente al valor de una clave criptográfica o de sus componentes cuando es necesario, al haberse destruido de sin justificación aparente.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.5.2. Se accede a información confidencial, al acceder a los valores de una clave o componente de clave criptográfica que no fue destruida o cuya destrucción se realizó de manera inadecuada.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.5.3. Se accede a información confidencial, al no verificar que la clave o componente de clave criptográfica que la encriptaba, haya sido destruida de manera que dicha clave o componente no pueda ser reconstruida.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.5.4. Se accede a información confidencial, al acceder a los valores de una clave o componente de clave criptográfica que fue destruida en uno o más ambientes y/o formatos donde se encontraba almacenada, pero no en todas sus ubicaciones y/o formatos.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.5.5. Se accede a información confidencial, al no poder eliminar o cambiar el valor de una clave criptográfica cuya seguridad ha sido comprometida.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.5.6. Se accede a información confidencial, al no eliminar de manera adecuada las claves o componentes de clave criptográficas, cuando los equipos y/o terminales que utilizaban dichas claves ya no son utilizados.

Probabilidad: Baja Impacto: Medio Criticidad: Media

4.2.6 Almacenamiento

R1.6.1. La clave LMK es almacenada en equipos que no cuentan con un nivel de seguridad adecuado, que obligue el acceso a la misma sólo bajo control dual.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.6.2. Se accede a información privada de clientes o del Banco, por control inadecuado del acceso, acceso no restringido o acceso sin control dual a las claves KEK o claves de trabajo.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.2.7 Respaldo

R1.7.1. Se pierde información o no se puede acceder a la misma ante la pérdida o destrucción de las claves criptográficas o de los equipos que las contienen, por no contar con respaldo electrónico de dichas claves.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.7.2. Se pierde información o no se puede acceder a la misma ante la pérdida o destrucción de los componentes de las claves criptográficas respectivas, por no contar con respaldo de dichos componentes en una ubicación alterna.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.7.3. Se accede a información privada de clientes o del Banco, al acceder a claves o componentes de claves criptográficas de respaldo, que no cuentan con controles de seguridad adecuados.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

4.2.8 Custodia

R1.8.1. No es posible identificar al custodio de un componente de clave criptográfica.

Probabilidad: Media Impacto: Medio Criticidad: Media

R1.8.2. Un custodio de componente de clave criptográfica no mantiene adecuadamente la confidencialidad de la misma, al no conocer con precisión las responsabilidades que la custodia conlleva.

Probabilidad: Media Impacto: Medio Criticidad: Media

R1.8.3. No es posible identificar las actividades de un custodio en relación con el componente de clave criptográfica que éste custodia.

Probabilidad: Baja Impacto: Medio Criticidad: Media

R1.8.4. No es posible acceder a un componente de clave criptográfica cuando es necesario, por no encontrarse disponible su custodio.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R1.8.5. Se compromete la integridad y/o confidencialidad de una clave criptográfica, al retirarse su custodio de la institución.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R1.8.6. Se compromete la integridad y/o confidencialidad de una clave criptográfica, al acceder su custodio al componente de clave criptográfica respectiva sin autorización y/o supervisión.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

4.3 De las Claves Criptográficas en papel

4.3.1 Generación

R2.1.1. Los componentes de claves en papel, son conocidos por personal distinto a su custodio, por no ser registrado por el propio custodio.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R2.1.2. Las claves criptográficas en papel, son conocidos por personal distinto al de la División Seguridad de Información, por no ser registrado por dicho personal.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R2.1.3. Se accede a información privada de clientes o del banco, por registrar en medios no seguros, el valor en claro de una clave criptográfica.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.1.4. Se accede a un componente de clave criptográfica, por no identificar al custodio respectivo.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R2.1.5. No se identifica una clave o componente de clave vigente en el sistema, ya que no se marcan o nombran adecuadamente los mismos.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.1.6. No se identifica una clave o componente de clave de producción, ya que no se marcan o nombran adecuadamente aquellos que pertenecen a desarrollo, pruebas y producción.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.1.7. No se identifica una clave o componente de clave por canal, ya que no se marcan o nombran adecuadamente los mismos.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.3.2 Reemplazo

R2.2.1. No se identifica el componente de clave criptográfica vigente, al no reemplazar de manera adecuada los formatos impresos de dichos componentes.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.3.3 Transporte

R2.3.1. Se accede a información privada de clientes o del banco, por enviar de manera impresa claves o componentes de claves a otra institución.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

4.3.4 Destrucción

R2.4.1. Se accede a información privada de clientes o del Banco, por no destruir adecuadamente las claves o componentes de claves criptográficas registradas en papel.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.4.2. No se identifica el formato de componente de clave vigente en el sistema, al no destruirse el componente en papel que ya no se encuentra vigente.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.3.5 Almacenamiento

R2.5.1. Se accede a claves o componentes de claves criptográficas en papel, por no almacenarse los formatos de manera adecuada.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.5.2. Se accede a claves o componentes de claves criptográficas en papel, por acceder personas ajenas a los formatos almacenados en cajas de seguridad.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.5.3. Se pierde información de claves o componentes de claves, al almacenarse todos los formatos en una misma ubicación o local.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R2.5.4. No se puede acceder oportunamente a un componente de clave criptográfica, al no encontrarse disponible el custodio respectivo.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R2.5.5. No es posible identificar las actividades realizadas con un formato de componente de clave criptográfica.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.3.6 Respaldo

R2.6.1. Se accede a información privada de clientes o del banco, por no contar las copias de respaldo con los mismos controles de los formatos principales.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.3.7 Custodia

R2.7.1. Se pierde información de claves o componentes de claves criptográficas, por no contar con respaldos de las mismas en papel.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R2.7.2. Se pierde información de claves o componentes de claves criptográficas, por no controlar la salida de los custodios respectivos de la institución.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R2.7.3. Se pierde información de claves o componentes de claves criptográficas, al cambiar de puesto los custodios respectivos, y no definirse la continuidad de la custodia.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.4 Del Coprocesador Criptográfico

4.4.1 De la Generación de llaves

R3.1.1. Se compromete la información privada de clientes o del Banco, al ingresar los componentes de llaves criptográficas en la aplicación del coprocesador que no cuenta con controles de acceso adecuados.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R3.1.2. Se compromete la información privada de clientes o del Banco, al acceder personas ajenas a los archivos del coprocesador criptográfico que contienen las llaves criptográficas.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R3.1.3. No se puede validar o encriptar información privada de los canales de atención conectados al coprocesador, al perderse el valor de las llaves almacenadas en la base de datos compartida por el coprocesador principal y el de respaldo.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R3.1.4. Se accede a información privada de clientes o del Banco, al compartir información entre los HSM, Switch Stratus y el coprocesador criptográfico.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R3.1.5. Se ingresa una llave criptográfica incorrecta al no poder verificar su valor de chequeo.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

4.4.2 De la restauración

R3.2.1. No se puede restituir una llave criptográfica, al no haber podido verificar el ingreso correcto de un componente de llave criptográfica a través de su valor de chequeo.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.5 De la Banda Magnética

R4.1.1. Terceras personas acceden a información privada de clientes, al clonar los datos de la banda magnética de sus tarjetas.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

4.6 Del Algoritmo DES

R5.1.1. Terceras personas acceden a información privada de clientes, al interceptar y decodificar información encriptada bajo al algoritmo DES.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

4.7 De los HSM

R6.1.1. Se pierde información de claves criptográficas al no instalarse los equipos de almacenamiento de las mismas, en ubicaciones seguras, bajo condiciones adecuadas.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R6.1.2. No se puede validar información encriptada por no encontrarse disponibles los HSM en una contingencia, si se encuentran instalados en la misma ubicación.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R6.1.3. Se accede a información confidencial al utilizarse medios inseguros para el acceso a los equipos criptográficos.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R6.1.4. No es posible identificar las acciones realizadas con los HSM.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R6.1.5. Se accede a información de claves criptográficas por tener el acceso a las funciones de los equipos de criptografía una sola persona.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R6.1.6. Se accede a información de claves criptográficas por tener el acceso a las funciones de los equipos de criptografía sin justificación y/o autorización.

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.8 De la grabación de tarjetas

R7.1.1. Se accede a información confidencial de las tarjetas, por el acceso a las claves criptográficas durante el proceso de grabación de tarjetas.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R7.1.2. Se accede a información confidencial de las tarjetas, por no controlar el acceso a las funciones o área de grabación de las mismas.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R7.1.3. Se pierde información interna del banco por perderse o hacer mal uso de tarjetas antes, durante y/o después del proceso de grabación.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R7.1.4. Se accede a información confidencial de tarjetas, por realizar el envío de datos para su generación en texto plano.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

R7.1.5. Se accede a información confidencial por no destruir de manera segura las tarjetas con algún tipo de daño en el proceso de grabación

Probabilidad: Media Impacto: Alto Criticidad: Alta

4.9 De la operación

R8.1.1 Se accede a información de clientes, por procesarse dicha información en equipos no seguros.

Probabilidad: Media Impacto: Alto Criticidad: Alta

R8.1.2 Se accede a información de clientes, por almacenarse dicha información en texto claro.

Probabilidad: Baja Impacto: Alto Criticidad: Alta

R8.1.3. No es posible realizar tareas con las claves criptográficas por no contar con procedimientos documentados, validados y actualizados para realizar dichas tareas.

Probabilidad: Alta Impacto: Alto Criticidad: Alta

Capítulo 5: Controles de seguridad de información para las claves criptográficas de los ATMs del Banco de la Nación

La administración de llaves juega un rol esencial en la integración de componentes de una arquitectura de seguridad de trabajo. Este provee soporte de seguridad crítico para el siclo de vida de la tarjeta y el procesamiento de transacciones para asegurar la integridad de todos los procesos criptográficos. La seguridad de datos es dependiente de la prevención de revelación y modificación, substitución, inserción o eliminación de llaves no autorizada.

En esta sección se identifican los controles que se deben implementar para elevar el nivel de confidencialidad, integridad, disponibilidad, autentificación y no repudio de la información utilizada en operaciones en cajeros automáticos o ATMs del Banco de la Nación, de acuerdo a los riesgos identificados en el Capítulo anterior.

Para ello, cada control indicará el riesgo o riesgos que mitigarían si son implementados de manera adecuada, señalados con el término *"Riesgos mitigados"*.

5.1 De las Claves Criptográficas

5.1.1 Generación

- Las claves criptográficas utilizadas para la encriptación y desencripción de datos se deben crear utilizando procesos que aseguren que no sea posible predecir ninguna clave ni determinar que determinadas claves son más probables que otras. Dichas claves y componentes de claves se deben generar utilizando un proceso aleatorio.

Para cumplir con este control es necesario que todo componente de claves criptográfica del Banco de la Nación provenga de un valor generado en los HSM.

Riesgos mitigados: 1.1.1, 1.1.2,

- Todo componente de clave criptográfica maestra o KEK almacenado electrónicamente, debe ir acompañado de su respectivo valor de chequeo, para comprobar que el ingreso de llaves ha sido adecuado, y verificar la autenticidad de la misma.

  Riesgos mitigados: 1.1.1, 1.1.3, 1.1.11

La generación de las claves y componentes de claves se realizará siempre en los equipos HSM, los cuales aseguran que el proceso de generación de componentes es aleatorio, de acuerdo a lo establecido por el estándar EMV [Thales07].

La División Seguridad de Información deberá revisar periódicamente que el generador de números aleatorios de los HSM se encuentre en buen estado, a través del comando DT, como se muestra en la tabla 5.1:

Diagnostic Test

Command: DT (Diagnostic Test). The HSM must be offline or in the secure state.

Function: To perform diagnostic tests.
The DT command tests the following parts of the HSM:

- Working memory areas (RAM).
- Program code.
- The DES cryptographic processor.
- Smartcard reader operation.
- The RSA cryptographic processor.
- Battery voltage level.

Inputs: None.

Outputs: PASS or FAIL messages.

Errors: None.

Example:

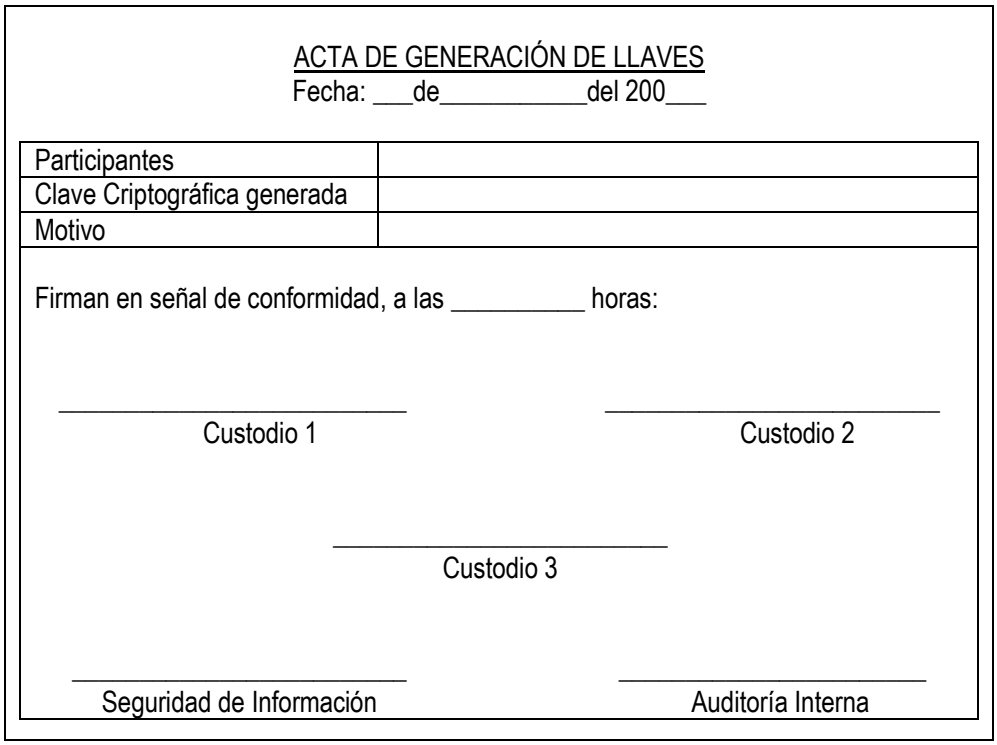
```
Offline>dt
Memory test...OK
Firmware test...OK
DES test...OK
Check smartcard eject...
Cryptographic test... OK
Battery...OK
Random Number Generator test...
   Monobit...OK
   Poker...OK
   Runs...OK
   Long Run...OK

Diagnostics complete
```

Tabla 5.1. Comandos de diagnóstico del HSM 8000 [Thales04]

Riesgos mitigados: 1.1.1, 1.1.2, 1.1.3

- Para no comprometer la seguridad del proceso de generación de claves, esta labor debe realizarse con por lo menos la participación de dos custodios por clave criptográfica.

  La División Seguridad de Información debe ser la encargada de verificar que cada componente sea generado por custodios diferentes. Para ello cada generación o restauración de llave criptográfica debe ir acompañado de un Acta de Generación de Llaves, firmado tanto por los custodios, Seguridad de Información y Auditoría Interna, tal como se muestra en la figura 5.1:



ACTA DE GENERACIÓN DE LLAVES
Fecha: ___de_____del 200___

Participantes	
Clave Criptográfica generada	
Motivo	

Firman en señal de conformidad, a las _____ horas:

_____ Custodio 1

_____ Custodio 2

_____ Custodio 3

_____ Seguridad de Información

_____ Auditoría Interna

Figura 5.1. Acta de Generación de Llaves

Riesgos mitigados: 1.1.3

- La llave maestra y las llaves KEK, por estar sujetas a un mayor riesgo, deberán ser generadas con por lo menos tres componentes custodiados por tres personas distintas.

  Riesgos mitigados: 1.1.3

- Los componentes de claves no encriptadas se introducen sólo en los HSM y en los ATM para generar las respectivas claves criptográficas, utilizando los

principios de control dual y conocimiento compartido, por sus respectivos custodios debidamente identificados.

Riesgos mitigados: 1.1.3, 1.1.7

- Todo el hardware y todas las contraseñas utilizadas para generar y/o cargar las claves criptográficas se deben administrar bajo control dual.

  Riesgos mitigados: 1.1.9, 1.1.13

- La carga de las claves o de los componentes de clave incorpora un mecanismo de validación tal que la autenticidad de las claves está garantizada y se pueda determinar que las mismas no han sido alteradas, sustituidas o comprometidas en forma alguna, a través de la verificación del valor de chequeo.

  Riesgos mitigados: 1.1.1, 1.1.2, 1.1.3, 1.1.11

- Todas las claves criptográficas utilizadas por un terminal que origina transacciones y procesa PINs son únicas para cada terminal.

  Riesgos mitigados: 1.2.1, 1.2.2

- Las claves criptográficas del Banco sólo se almacenan en el HSM, en el switch central de ATMs, en tokens o en formatos impresos, con acceso de forma segura, utilizando los principios de control dual y conocimiento compartido, así como los controles de acceso físico y lógico especificados en el presente trabajo.

  Riesgos mitigados: 1.6.1, 1.6.2, 1.1.5, 1.1.6

- Se requieren controles duales de acceso para habilitar las funciones de encriptación de claves.

  Riesgos mitigados: 1.1.3, 1.1.12

- Para disminuir el impacto de compromiso de las llaves criptográficas de los cajeros automáticos, se debe implementar el uso del PVKI, del 1 al 6, por cada 5000 tarjetas emitidas.

  Riesgos mitigados: 1.1.4

- La información confidencial de clientes y del banco debe estar encriptada bajo el estándar EMV, utilizando infraestructura de llaves públicas.

Riesgos mitigados: 1.1.8, 4.1.1, 5.1.1

5.1.2 Segregación

La segregación es necesaria para limitar la magnitud y el impacto que generaría la exposición de la información de los clientes o del banco, en caso de verse comprometida la seguridad de alguna clave o componente de clave criptográfica.

- Las claves de encriptación se deben usar solamente para el propósito para el cual se generaron y solamente para un canal. Esto significa que una clave de encripción no debe generarse nunca a partir de componentes de clave que pertenecen a otra clave de encripción. Por ejemplo: las claves de terminal TMK no deben generar a partir de los mismos componentes de las claves de encripción del PIN (PVK). Así mismo, la clave de encripción de zona ZMK utilizada en la comunicación con VisaNet Perú no debe generarse a partir de los mismos componentes de la clave de encripción de zona ZMK utilizada en la comunicación con Visa Internacional.

  Riesgos mitigados: 1.2.1, 1.2.2

- Las claves criptográficas no se deben compartir ni sustituir nunca entre los ambientes, computadores y/o HSM de desarrollo, prueba, producción y otro ambiente equivalente.

  Riesgos mitigados: 1.2.3

5.1.3 Reemplazo

- Las claves y componentes de claves que ya no se usan o se han reemplazado, deben destruirse forma segura.

  Riesgos mitigados: 1.3.3, 1.3.4

- Los componentes de clave nunca se deben cargar nuevamente en los HSM, si hay alguna sospecha de que se ha comprometido la seguridad de dichos componentes o del equipo HSM.

Riesgos mitigados: 1.3.1, 1.3.2, 1.3.4

- De tener sospecha de que algún equipo HSM ha sido alterado, los componentes de claves a reingresar o nuevos componentes de claves no deben ser ingresados hasta que el equipo haya sido reemplazado o inspeccionado y se tenga una garantía de que el equipo no ha estado sujeto a una modificación física o funcional no autorizada.

  Riesgos mitigados: 1.3.3

- De tener sospecha de que una clave ha sido comprometida, dicha clave criptográfica debe sustituirse con una nueva clave. Todas las claves derivadas de dicha clave a ser reemplazada, deben reemplazarse con una nueva clave inmediatamente. Todas las claves encriptadas bajo dicha clave a ser reemplazada deben ser reencriptadas una vez que la clave haya sido reemplazada.

  Riesgos mitigados: 1.3.1, 1.3.2, 1.3.4

- Los componentes de la nueva clave criptográfica de reemplazo no deberán ser variantes ni transformaciones de los componentes originales a ser reemplazados.

  Riesgos mitigados: 1.3.2, 1.3.4

- Una vez generada la nueva clave, se debe proceder con la destrucción de la clave original y todas las variantes y transformaciones no reversibles de la misma, así como de todas las claves encriptadas o derivadas de esa clave.

  Riesgos mitigados: 1.3.1, 1.3.2, 1.3.4

5.1.4 Transporte

- Las claves criptográficas privadas que sean transportadas a través de una línea de comunicación y cuya función no sea el de encriptar información que viaje a través de la red (como PVK o CVK), deben estar encriptadas bajo una clave de zona, IWK, AWK o TMK públicas, según sea el caso.

  Riesgos mitigados: 1.4.1, 1.4.2, 1.4.3

- Los componentes de claves criptográficas no deben ser transportadas por una línea de comunicación en texto plano. Éstas deberán encontrarse encriptadas bajo una clave de zona IWK, AWK o TMK, según sea el caso.

  Riesgos mitigados: 1.4.1, 1.4.2, 1.4.3

- Cualquier componente de clave que no se encuentre encriptado ni almacenado en un HSM o un token, estará en todo momento durante su transmisión o movimiento entre el Banco y Visa Internacional, bajo la supervisión continua de su custodio, el cual ser debidamente identificado, previo al acceso al componente.

  Riesgos mitigados: 1.4.3

5.1.5 Destrucción

- La destrucción de una clave deberá realizar en caso se detecte conocimiento o acceso de la misma por parte de terceros, por cambio de la clave de la cual se derivó, o por desuso de la misma. Este control deberá ser expresamente autorizado por la División Seguridad de Información y respaldado por el Departamento de Informática y Auditoría Interna.

  Riesgos mitigados: 1.5.2

- En todos los casos en que sea necesaria la destrucción de una clave o componente de clave criptográfica, un tercero que no sea el custodio (Auditoría Interna o Asesoría Legal) deberá observar el procedimiento de destrucción, dando fe de que dicha clave ha sido destruida de acuerdo a los estándares establecidos en este documento, y que dicha clave no puede ser reconstruida de ninguna forma.

  Riesgos mitigados: 1.5.3, 1.5.6

- La finalización del ciclo de vida de la clave ocurre cuando todas las instancias de la clave en todas las formas permitidas son destruidas, abarcando todas las locaciones (operacional, backup, almacenamiento) donde exista dicha clave.

  Riesgos mitigados: 1.5.4

- No debe existir información a través de la cual se pueda derivar el valor de una clave o componente de clave criptográfica que haya sido destruida.

  Riesgos mitigados: 1.5.2, 1.5.3

- Las claves criptográficas almacenadas en un HSM, deberán ser eliminadas a través del siguiente comando: CS Configure Security, donde es necesario borrar el valor de la LMK por seguridad:

Configure Security

Command:	CS (Configure Security). The HSM must be in the Secure state.
Function:	To set the security configuration of the HSM and some processing parameters. CS converts all lower-case alpha values to upper case for display purposes, except for the Card issuer Password. Operation is menu-driven, as shown in the examples. The security settings can optionally be saved to a Smartcard.
Inputs:	PIN length [4-12]: a one or two-digit number in the range 4 to 12. Echo [oN/ofF]: N or F Atalla ZMK variant support [oN/ofF]: N or F Transaction key scheme: Racal, Australian or None? [R/A/N]: R or A or N User storage key length [S/D/T]: S, D or T Erase LMKs? [Y/N]: confirm Y or N Select clear PINs? [Y/N]: Y or N Enable ZMK translate command? [Y/N]: Y or N Enable X9.17 for import? [Y/N]: Y or N Enable X9.17 for export? [Y/N]: Y or N Solicitation batch size [1-1024]: a one to four-digit number, range 1 to 1024 Enable Single-DES [Y/N]: Y or N Prevent Single-DES keys masquerading as double or triple-length key? [Y/N]: Y or N Single/double length ZMKs [S/D]: S or D (Single or Double) Decimalization table Encrypted/Plaintext [E/P]: E Enable decimalization table checks? [Y/N]: Y or N PIN encryption algorithm: A or B (Visa method or Racal Method) Card/password authorisation [C/P]: C or P (Card or Password) Card issuer password [ENTER = no change]: 8 alphanumeric printable characters Authorised State required when importing DES key under RSA key? [Y/N]: Y or N Minimum HMAC verification length in bytes [5-20]: a one to two-digit number, range 5-20 Enable PKCS#11 import and export for HMAC keys [Y/N]: Y or N Enable ANSI X9.17 import and export for HMAC keys [Y/N]: Y or N Enable ZEK encryption of all printable ASCII chars [Y/N]: Y or N Enable ZEK encryption of "Base94" ASCII chars [Y/N]: Y or N Enable ZEK encryption of "Base64" ASCII chars [Y/N]: Y or N Enable ZEK encryption of "Hex-only"ASCII chars [Y/N]: Y or N Restrict Key Check Values to 6 hex chars [Y/N]: Y or N Enable Multiple Authorised Activities [Y/N]: Y or N Save SECURITY settings to Smartcard? [Y/N]: Y or N

Tabla 5.2. Comandos de configuración de seguridad del HSM 8000 [Thales04]

En la opción 'Erase LMKs?' se deberá ingresar la opción 'Y' Yes (ver tabla 5.1)

Para verificar que la LMK ha sido eliminada, se ingresará a la opción 'V' Verifying the Contents of the LMK Store (ver tabla 5.3):

Verifying the Contents of the LMK Store

Command:	V (Verify). Can be used in online, offline or secure state.
Function:	To confirm that the check value is identical to the value that was recorded when the LMK set was installed.
Inputs:	None.
Outputs:	Master key check value.
Errors:	None.

Example:

```
Online> V <Return>
Check: XXXX XXXX XXXX XXXX
```

Tabla 5.3. Comandos de visibilidad de LMK del HSM 8000 [Thales04]

El valor CHECK mostrará '0000 0000 0000 0000'. Cabe resaltar que el valor de la LMK no es visible para ninguna persona, sólo es posible visualizar su valor de chequeo.

Esta labor deberá estar a cargo de la División Seguridad de Información y los custodios de las llaves físicas, con la presencia de personal de Auditoría y los custodios de la LMK.

Riesgos mitigados: 1.5.2, 1.5.3

- Los componentes de claves almacenadas en tokens deberán ser borradas a través del siguiente comando: FC Format SmartCard (ver tabla 5.4)

Formatting a Smartcard

Command:	FC (Format Card). Can be used in online, offline or secure state.
Function:	To format a Smartcard for use by the HSM. Different formats are used for LMK storage and saving HSM settings.

```
Online> FC <Return>
Insert card and press ENTER: <Return>
Card already formatted, continue? [Y/N]: Y <Return>
Format card for HSM settings/LMKs? [H/L]: L <Return>
  Erasing card
  Formatting card . . .
Enter new PIN for Smart Card: ******* <Return>
Re-enter new PIN: ******* <Return>
Enter time [hhmmss]: 153540 <Return>
Enter date [ddmmyy]: 261093 <Return>
Enter User ID: Joe Small <Return>
Enter Issuer ID: Big Bank plc <Return>
Format complete
```

Tabla 5.4. Comandos de formateo de tarjetas del HSM 8000 [Thales04]

Riesgos mitigados: 1.5.2, 1.5.3, 1.5.6

- Las claves inscritas en el computador central, así como en el Switch Central de ATMs, al ser destruidas, deberán ser sobrescritos con 0s, como mínimo tres veces, por personal de la División Seguridad de Información, y en presencia de personal de Auditoría y de los custodios de las claves respectivas.

  Riesgos mitigados: 1.5.2, 1.5.3, 1.5.6

- Las claves inscritas en el switch de Visa Internacional y/o de Visanet Perú que se necesite sean eliminadas, serán notificadas a dichas instituciones. El proceso de borrado deberá cumplir como mínimo con los mismos controles establecidos dentro del Banco de la Nación.

  Riesgos mitigados: 1.5.2, 1.5.3, 1.5.5

- Las claves criptográficas inscritas en los cajeros automáticos que se necesite sean eliminadas, serán sobrescritos sus componentes con 0s. Este proceso se seguirá también en los casos en que el cajero automático vaya a ser desactivado, de manera temporal o definitiva.

  Riesgos mitigados: 1.5.2, 1.5.3, 1.5.5, 1.5.6

- Toda destrucción de componentes y de llaves criptográficas deberá ser registrada en un Acta de Destrucción de Componentes, firmada por los custodios, Personal de la División Seguridad de Información y de Auditoría Interna, según muestra la figura 5.2:

ACTA DE DESTRUCCIÓN DE COMPONENTES

Fecha: ___de_____del 200___

Participantes	
Clave Criptográfica a destruir	
Motivo de destrucción	

Firman en señal de conformidad, a las _____ horas:

_____ Custodio 1

_____ Custodio 2

_____ Seguridad de Información

_____ Auditoría Interna

Figura 5.2. Acta de Destrucción de Componentes

Riesgos mitigados: 1.5.1, 1.5.2, 1.5.3, 1.5.4, 1.5.5, 1.5.6

5.1.6 Almacenamiento

- La clave LMK sólo podrá estar almacenada en un equipo HSM.

  Riesgos mitigados: 1.6.1, 1.6.2

- Las claves KEK y las claves de trabajo privadas sólo podrán ser almacenadas de manera encriptada, en equipos con acceso lógico y físico restringido.

  Riesgos mitigados: 1.6.2

- Las claves públicas deben existir sólo en certificados digitales.

  Riesgos mitigados: 1.6.2

5.1.7 Respaldo

- Deben existir copias de respaldo de claves en una ubicación alterna solamente para el propósito de restituir las claves que accidentalmente se destruyan.

  Riesgos mitigados: 1.7.1, 1.7.2

- Toda clave y componente de clave criptográfica debe contar con un respaldo electrónico, que permita continuar con la validación de la información de los cajeros automáticos, en caso de presentarse una contingencia.

  Riesgos mitigados: 1.7.1, 1.7.2

- Deben existir copias de respaldo de los componentes de claves en una ubicación alterna solamente para el propósito de restituir una clave que accidentalmente se destruya, o para reencriptar una clave cuya clave KEK ha sido substituida.

  Riesgos mitigados: 1.7.1, 1.7.2

- Deben existir equipos de respaldo que soporten las claves y componentes de claves criptográficas, en una ubicación alterna.

  Riesgos mitigados: 1.7.1, 1.7.2

- Las copias de respaldo de las claves y componentes de claves criptográficas deben estar sometidas como mínimo a los mismos controles de las claves y componentes de las claves criptográficas principales.

  Riesgos mitigados: 1.7.3

5.1.8 Custodia

- La designación de los componentes de clave debe estar documentada y cada custodio debe firmar un Acta de Custodia del Componente de Clave. Dichos formularios deben autorizar e identificar específicamente las responsabilidades del custodio para salvaguardar los componentes de clave y otros materiales relacionados con el ingreso de los datos que se les confíen.

  Riesgos mitigados: 1.8.1, 1.8.2, 1.8.5

- A continuación en la figura 5.3, se presenta el modelo de Acta de Custodia:

ACTA DE CUSTODIA

N° Acta :
Clave Criptográfica :
Número de Componente :
Nombre del Custodio :
Tipo de Custodio :
Cargo del Custodio :
Teléfono :
Celular :
Fecha :

- Se denomina custodio a la persona encargada de resguardar un componente de la clave criptográfica de seguridad que se le ha confiado.

- Se encuentra considerado como una prohibición para los custodios, la infracción de cualquiera de las normas que a continuación se consignan.
  1. El custodio no deberá entregar o prestar información sobre el componente que está bajo su custodia con anterioridad, en el transcurso o posteriormente a la inscripción de la clave criptográfica.
  2. El custodio deberá verificar la recepción del componente de la llave que se encuentre en el sobre lacrado, manteniéndolo en un lugar seguro hasta su inscripción.
  3. Para los procesos de inscripción, el componente de la llave, sólo será extraído de su sobre por el custodio.
  4. El custodio deberá presenciar el procedimiento de destrucción del componente que está bajo su custodia, cuando este procedimiento sea requerido.
  5. Será de responsabilidad del custodio si un componente de la clave es conocido por otra persona y es su deber comunicar a la División de Seguridad de Información si existe la sospecha de que el componente que está bajo su custodia es conocido por un tercero no autorizado.

- En el caso en que deje de laborar en el Banco, no deberá divulgar el componente de la llave que estuvo bajo su custodia.

_____
Firma del Custodio

Figura 5.3. Acta de Custodia

Riesgos mitigados: 1.8.1, 1.8.2, 1.8.5

- El Acta de Custodia debe ser firmada en original y copia: una será almacenada por la División Seguridad de Información, y la otra resguardada por su respectivo custodio.

  Riesgos mitigados: 1.8.1, 1.8.2, 1.8.5

- Se deben mantener registros o bitácoras para documentar el acceso, retiro o reingreso de las claves, componentes de clave, tokens o llaves físicas. Estas bitácoras deben estar almacenadas físicamente en bóveda.

Riesgos mitigados: 1.8.3, 1.8.6

- Ningún custodio podrá tener acceso a su componente, sin haber sido solicitado por el Jefe de la División Seguridad de Información al Jefe de División Caja y Valores (Oficina Principal) o al Administrador de Agencia (Oficina de Respaldo).

  Riesgos mitigados: 1.8.3, 1.8.6

- Ningún custodio podrá tener acceso a su componente, sin ser supervisado directamente por personal de la División Seguridad de Información.

  Riesgos mitigados: 1.8.3, 1.8.6

- Todo custodio de clave criptográfica debe contar con un custodio de respaldo, cuyo componente debe almacenarse en el sitio de respaldo.

  Riesgos mitigados: 1.8.4

- En caso no encontrarse disponible el custodio principal de un componente de llave criptográfica, el custodio de respaldo deberá ocupar su lugar, a través del uso del respetivo componente de respaldo.

  Riesgos mitigados: 1.8.4

5.1.9 De la Operación

- Todos los PINes ingresados por el tarjetahabiente se deben procesar en los equipos HSM.

  Riesgos mitigados: 1.1.10, 8.1.1

- Los PINes no deben aparecer nunca en texto claro fuera del HSM.

  Riesgos mitigados: 1.1.10, 8.1.2

- Todos los PINes de tarjetahabientes procesados en línea se encriptan en el ATM bajo la llave TPK creada por los HSM.

  Riesgos mitigados: 1.1.10, 8.1.1

- Todos los procedimientos de generación, verificación, reemplazo, destrucción y otros relacionados a la administración de las claves criptográficas deberán estar debidamente documentados.

  Riesgos mitigados: 8.1.3

- La documentación de la administración de las claves criptográficas deberá ser validada y aprobada por la División Seguridad de Información, el Departamento de Planeamiento y Desarrollo y la Gerencia General, adicionalmente a las políticas de aprobación de directivas vigente del Banco de la Nación.

  Riesgos mitigados: 8.1.3

- Se debe poder demostrar que los procedimientos establecidos y documentados se están utilizando para procesar todas las operaciones de administración de claves.

  Riesgos mitigados: 8.1.3

- Toda la documentación de administración de llaves criptográficas debe ser actualizada periódicamente, o debido a cambios en los procesos o tecnología, por la División Seguridad de Información. Esta actualización debe estar reflejada en la versión respectiva de cada documento.

  Riesgos mitigados: 8.1.3

- El acceso a las funciones de los HSM se realizará a través de una consola dedicada sólo para dicha función.

  Riesgos mitigados: 6.1.3

- La consola de acceso a los HSM será administrada por la División Seguridad de Información.

  Riesgos mitigados: 6.1.3

- Todas las operaciones realizadas con la consola deberán ser registradas en un log.

  Riesgos mitigados: 6.1.4

- Todo acceso a la consola deberá ser registrado en una Bitácora de Accesos a la Consola de Administración de los HSM, según se muestra en la figura:

BITÁCORA DE ACCESOS A LA CONSOLA DE ADMINSTRACIÓN DE HSM
OFICINA

Fecha	Hora de acceso	Hora de fin	Responsable	Motivo	Firma

Figura 5.4. Bitácora de Accesos a la Consola de Administración de los HSM

Riesgos mitigados: 6.1.4, 6.1.6

- Deberá existir una consola en cada ubicación de los HSM, es decir, una en la Oficina Principal y una en la Oficina de Respaldo. Estas consolas no deben estar conectadas permanentemente a los HSM, sino almacenadas en las respectivas bóvedas de seguridad de cada una de las oficinas.

  Riesgos mitigados: 6.1.2, 6.1.3, 6.1.5

- La bóveda de seguridad donde se almacenan las cajas de seguridad y las consolas debe ser accedida bajo los principios de control dual y conocimiento compartido.

  Riesgos mitigados: 6.1.5

5.2 De las Claves Criptográficas en papel

5.2.1 Generación

- Las componentes de claves criptográficas que requieran ser registrados en papel, deberán estar escritos sólo por su custodio, en formatos estándares, donde se registre la clave criptográfica a la cual pertenece, el número de componente, el nombre del custodio, canal de atención relacionado, el valor en claro del componente, el valor de chequeo, y la fecha de generación.

  Riesgos mitigados: 2.1.1, 2.1.5, 2.1.7

- Las claves criptográficas que requieran ser registradas en papel, deberán ser escritas sólo por personal de la División Seguridad de Información, en

formatos estándares, donde se registre el nombre de la clave criptográfica, canal de atención relacionado, el valor encriptado de la clave, el valor de chequeo, y la fecha de generación.

Riesgos mitigados: 2.1.2, 2.1.5, 2.1.7

- No se debe almacenar nunca de manera escrita, el valor en claro de una clave criptográfica LMK. Éstas se almacenarán sólo en una tarjeta inteligente o token.

  Riesgos mitigados: 2.1.3

- Todo componente de llave KEK que sea registrado en papel, deberá ser almacenado en una caja de seguridad con llave física, entregada a su respectivo custodio.

  Riesgos mitigados: 2.1.3

- Ninguna persona podrá tener acceso a las claves o componentes de claves criptográficas registradas de manera escrita, el cual es limitado sólo a su respectivo custodio.

  Riesgos mitigados: 2.1.4

- Todo formato que registre una clave o componente de clave criptográfica, debe mantenerse dentro de un sobre lacrado, firmado en la tapa por el custodio, y que identifique en su exterior el nombre de la clave, número de componente y nombre del custodio.

  Riesgos mitigados: 2.1.4, 2.1.5, 2.1.7

- Todo clave o componente de clave criptográfica debe identificar el ambiente al cual pertenece dicha clave o componente.

  Riesgos mitigados: 2.1.6

5.2.2 Reemplazo

- Los formatos de claves y/o componentes de claves criptográficas deben ser destruidos cuando dichas claves sean reemplazadas.

  Riesgos mitigados: 2.2.1

5.2.3 Transporte

- Una clave o componente de clave criptográfica no podrá ser nunca enviada de manera física a otro destino. Para ello se deberá registrar la clave o componente de clave de manera electrónica y enviada utilizando un certificado digital.

  Riesgos mitigados: 2.3.1

5.2.4 Destrucción

- Los formatos de claves y/o componentes de claves criptográficas que requieran ser destruidas, deben ser quemados.

  Riesgos mitigados: 2.4.1, 2.4.2

- La destrucción de un formato impreso debe ser registrado en un Acta de Destrucción, de manera similar a la destrucción de claves electrónicas.

  Riesgos mitigados: 2.4.1, 2.4.2

5.2.5 Almacenamiento

- Las claves y componentes de claves criptográficas privadas registradas en papel, deben ser almacenadas en cajas de seguridad, con chapa y llave por custodio.

  Riesgos mitigados: 2.5.1, 2.5.2

- La llave física de una caja de seguridad será entregada al custodio del componente respectivo, y una copia será almacenada en la bóveda del Banco como respaldo.

  Riesgos mitigados: 2.5.2, 2.5.4

- Las cajas de seguridad serán almacenadas en las cajas fuertes de la Oficina Principal y la Oficina de Respaldo según sea el caso.

Riesgos mitigados: 2.5.3

- El acceso a las cajas fuertes será solicitado sólo por el Jefe de la División Seguridad de Información o por el Gerente General, y será autorizado por el Jefe de la División de Caja y Valores (Oficina Principal) o por el Administrador de Agencia (Oficina de Respaldo).

  Riesgos mitigados: 2.5.1, 2.5.5

- En caso de emergencia, en los cuales no se encuentra el custodio de un componente, la Gerencia General podrá autorizar el acceso a dicho componente por parte del personal de la División Seguridad de Información, utilizando la llave de la caja de seguridad respectiva, almacenada en la bóveda del Banco.

  Riesgos mitigados: 2.5.4

- Todo acceso a componentes almacenados deberá ser registrado en una bitácora que se encuentre en la caja fuerte, indicando la fecha y hora de acceso, nombre del custodio, firma, motivo de acceso y hora de retorno del componente. El modelo de bitácora se muestra en la figura 5.5:

BITÁCORA DE ACCESOS A LA CAJA FUERTE
OFICINA_____

Fecha	Hora de acceso	Hora de retorno	Custodio	Motivo	Firma

Figura 5.5. Bitácora de Accesos a la Caja Fuerte

Riesgos mitigados: 2.5.2, 2.5.5

5.2.6 Respaldo

- Todas las copias de respaldo en papel deben estar sujetas al mismo o mayor nivel de seguridad sobre los formatos de claves principales.

  Riesgos mitigados: 2.6.1

5.2.7 Custodia

- Todo custodio debe contar con un custodio de respaldo, que pueda acceder a un componente de clave criptográfica almacenada en la Oficina de Respaldo.

  Riesgos mitigados: 2.7.1

- En caso un custodio se retire de la institución, deberá entregar la llave de la caja de seguridad respectiva a la División Seguridad de Información, que se encargará de reasignar los componentes y SmartCard (de ser el caso) a otro custodio.

  Riesgos mitigados: 2.7.2

- En caso un custodio cambie de cargo, el custodio o el Departamento de Personal deberá informar de dicho cambio a la División Seguridad de Información, para que lo registre en su cuadro de custodios. Mientras el custodio permanezca en la institución, a pesar del cambio de cargo, mantendrá la custodia del componente, para reducir el nivel de conocimiento de dicho componente.

  Riesgos mitigados: 2.7.3

5.3 Del Coprocesador Criptográfico

- Se debe migrar de manera paulatina todos los canales de atención que se validan en el coprocesador criptográfico, a ser validados por los HSM, siguiendo la lógica y controles establecidos para los cajeros automáticos.

  Riesgos mitigados: 3.1.1, 3.1.2, 3.1.3, 3.1.4

- Mientras se realicen trabajos de migración del coprocesador a los HSHM, o si la empresa decide no realizar dicha migración, el coprocesador debe permitir visualizar el valor de chequeo de los componentes y llaves criptográficas.

  Riesgos mitigados: 3.1.5, 3.2.1

- Así mismo, se debe implementar bases de datos independientes para cada coprocesador criptográfico.

  Riesgos mitigados: 3.1.3

5.4 De los HSM

5.4.1 Seguridad física

- Los HSM deberán estar instalados en racks con llave. Dichos racks deben contar con las condiciones de temperatura adecuadas, entre X y Y °C.

  Riesgos mitigados: 6.1.1

- Los racks deben estar instalados en los respetivos Centros de Cómputo, principal y de respaldo.

  Riesgos mitigados: 6.1.2

- Los HSM deberán estar configurados para generar alarmas de movimiento y temperatura, a través de una conexión serial, siguiendo los comandos de los HSM de la siguiente manera: CL Configure Alarms, según la tabla 5.4:

Configure the Alarms

The HSM alarm circuitry should be turned on when the HSM is put into service. The alarms typically need to be turned off if the HSM is to be moved.

The HSM must be in the secure state to configure the alarms.

Enter CL <Return> (Configure aLarms) to initiate the following example in which both the temperature alarm and the motion alarm are turned on. User input is shown underlined. The option to save the alarm settings to Smartcard is selected.

Example:

```
Secure> CL <Return>
LMKs must be erased before proceeding.

Erase LMKs? [Y/N]: Y <Return>
Temperature Alarm [oN/ofF]: F <Return>
Motion Alarm [oN/ofF]: F <Return>
Save ALARM settings to smart card? [Y/N]: Y <Return>

Insert card and press ENTER: <Return>
ALARM settings saved to the smart card.
```

Tabla 5.4. Comandos de configuración de alarmas del HSM 8000 [Thales04]

Se deberán ingresar las siguientes opciones:

- Temperature Alarm: Y (Yes)
- Motion Alarm: Y (Yes)

Se debe tener en cuenta que esta configuración debe realizarse luego de haber instalado físicamente los HSM en los Centros de Cómputo respectivos, ya que ante cualquier movimiento o cambio de temperatura, el valor de la LMK será borrada automáticamente de los HSM.

Riesgos mitigados: 1.1.10, 6.1.1

- La consola de los HSM deberá encontrarse almacenada en la caja de seguridad de la División Seguridad de Información y sólo podrá ser accesada para tal fin.

  Riesgos mitigados: 6.1.3

- Los HSM deberán ser monitoreados con cámaras de seguridad durante todo el día.

  Riesgos mitigados: 1.1.10, 6.1.1, 6.1.4

- El acceso autorizado a los HSM deberá registrarse en bitácoras de acceso que identifique los siguientes datos: persona que accede, fecha y hora de acceso, motivo de acceso, hora de fin de acceso y firma.

  Riesgos mitigados: 6.1.4

- El acceso a los HSM debe ser justificado por el Jefe de la División Seguridad de Información y autorizado por el jefe del área custodia de los centros de cómputo: en el caso del Centro de Cómputo Principal será el Jefe de Producción, y en el caso del Centro de Cómputo de Respaldo, será el Administrador de la Agencia San Borja.

  Riesgos mitigados: 6.1.3, 6.1.4

- El acceso a los HSM debe ser siempre bajo control dual.

  Riesgos mitigados: 6.1.5

5.4.2 Seguridad lógica

- El acceso a los HSM se realizará a través de una consola dedicada exclusivamente para tal fin.

  Riesgos mitigados: 6.1.3

- El acceso a la consola de los HSM deberá registrarse en bitácoras de acceso que identifique los siguientes datos: persona que accede, fecha y hora de acceso, motivo de acceso, hora de fin de acceso y firma.

  Riesgos mitigados: 6.1.4

- Sólo los custodios de las claves pueden tener acceso a los equipos HSM, cuando por razones justificadas y autorizadas necesiten obtener dicho acceso.

  Riesgos mitigados: 6.1.3, 6.1.4, 6.1.6

- El acceso de los custodios debe ser siempre justificado por el Jefe de la División Seguridad de Información al custodio del Centro de Cómputo respectivo.

  Riesgos mitigados: 6.1.6

- El acceso a las funciones de seguridad y configuración de los equipos HSM será realizado sólo por personal autorizado de la División Seguridad de Información.

  Riesgos mitigados: 6.1.3, 6.1.6

5.5 Grabación de tarjetas

5.5.1 Seguridad Física

- El área de grabación de las tarjetas debe estar distribuida de manera que las actividades de ingreso de tarjetas nuevas, así como la entrega de tarjetas grabadas, no deben interrumpir ni tener acceso a las actividades propias de la grabación de tarjetas.

  Riesgos mitigados: 7.1.1

- Las actividades del personal que realiza la entrega, grabación y salida de tarjetas deben estar monitoreadas constantemente, a través del uso de cámaras de seguridad que puedan capturar las actividades pero no los valores ingresados a los procesadores y/o máquinas embosadoras.

  Riesgos mitigados: 7.1.2

- Todo acceso de tarjetas en blanco y salida de tarjetas grabadas debe ser registrado en una bitácora que se encuentre en el área de grabación.

  Riesgos mitigados: 7.1.3

- El área de grabación de tarjetas debe ubicarse siempre en un área restringida, por lo que no debe contar con paredes, ventanas o puertas que colinden con la parte externa del edificio del Banco.

  Riesgos mitigados: 7.1.1, 7.1.2, 7.1.3

- El acceso a esta área debe estar debidamente autorizada. Los operadores del equipo, asistentes y jefe del área deberán contar con una identificación de acceso que debe ser portada de manera constante. Así mismo, deberán usar un método automático de verificación de identidad, como una tarjeta de proximidad o controles biométricos.

  Riesgos mitigados: 7.1.2

- El acceso de personas ajenas al área de grabación deberá ser solicitado de manera escrita y justificada por un Gerente de Departamento, Gerente General o Jefe de órgano de control, y sólo podrá ser autorizado por el Jefe del área de grabación, bajo la opinión de la División Seguridad de Información.

  Riesgos mitigados: 7.1.2

- Todo acceso de personal ajeno al área de grabación, debidamente autorizado, deberá ser registrado y acompañado en todo momento por personal propia del área, verificando que los visitantes no tengan acceso a información confidencial.

  Riesgos mitigados: 7.1.3

- Se deben contar con alarmas de movimiento, para evitar la intrusión de personas ajenas al área mientras ésta se encuentre vacía.

  Riesgos mitigados: 7.1.1, 7.1.2, 7.1.3

- Las cámaras de monitoreo debe estar siempre activas y almacenar la información de por lo menos sesenta (60) días de anterioridad.

  Riesgos mitigados: 7.1.1, 7.1.2

- El sistema de cámaras y las alarmas deberán contar con mantenimiento preventivo y su funcionamiento deberá ser sometido a pruebas de manera periódica.

  Riesgos mitigados: 7.1.1, 7.1.2

- Todas las tarjetas en blanco que sean entregadas al área de grabación, deben almacenarse en una caja fuerte o bóveda interna. Se debe contar con una cámara que monitoree las actividades de ingreso y salida a dicha caja fuerte o bóveda, pero no deberán registrar el ingreso de la clave secreta de apertura.

  Riesgos mitigados: 7.1.3

- El acceso a la caja fuerte o bóveda debe realizarse bajo control dual. La clave de acceso y la llave física deben ser administradas por personas diferentes que pertenezcan al área de grabación.

  Riesgos mitigados: 7.1.3

- La clave de la caja fuerte y bóveda debe ser cambiada cada treinta (30) días o cada vez que el custodio de la clave sea reemplazado.

  Riesgos mitigados: 7.1.3

5.5.2 Seguridad lógica

- El acceso a las máquinas de grabación de tarjetas debe ser mediante clave de acceso que cumpla con los siguientes controles:

  - Identificador único en la red
  - Identificador único en la aplicación de grabación de tarjetas

- La contraseña no debe ser menor de 8 dígitos
- La contraseña debe ser forzada a cambiarse como máximo cada 30 días.
- La contraseña deberá constar de por lo menos 2 de los siguientes grupos de caracteres: letras minúsculas, letras mayúsculas, números, caracteres especiales.
- La contraseña no podrá repetirse hasta por lo menos haber realizado 6 cambios de la misma.
- En caso de olvido de la contraseña, esta deberá ser restaurada a través del sistema de administración de contraseñas del Banco. De generarse una contraseña por defecto o que sea conocida por el administrador de la red, ésta deberá ser cambiada automáticamente por el operador.

Riesgos mitigados: 7.1.2

- Toda actividad realizada dentro de la aplicación, debe ser registrada por un log de auditoría, donde se especifique la hora, fecha y actividad realizada con un identificador de usuario. Los intentos fallidos de acceso también deberán ser registrados en el log.

  Riesgos mitigados: 7.1.2

5.5.3 Procesamiento

- El archivo que contiene la información de los tarjetahabientes, cuentas y llaves de seguridad, que es enviada desde el computador central hacia las máquinas de grabación de tarjetas, debe viajar por la red de manera encriptada bajo una llave ZPK.

  Riesgos mitigados: 7.1.4

- Se debe verificar de manera dual que el número de tarjetas a grabar sea igual al número de tarjetas solicitadas por el computador central. No se deben grabar tarjetas que no hayan sido solicitadas.

  Riesgos mitigados: 7.1.3

- Al finalizar el proceso, dos personas deben contar el número de tarjetas grabadas y sin grabar, para comprarlo con el número de tarjetas retiradas de

la caja fuerte o bóveda, y concordarlo con la orden de trabajo. Si existe alguna diferencia, debe revisarse si hay informe de tarjetas dañadas.

Riesgos mitigados: 7.1.3

- En caso que una tarjeta resulte dañada por el proceso, ésta deberá ser almacenada en la caja fuerte o bóveda, hasta que se indique el momento de destrucción de dicha tarjeta.

  Riesgos mitigados: 7.1.3

- La destrucción de las tarjetas debe realizarse de manera segura, que no permita reconstruir la información que en ella pudo almacenarse.

  Riesgos mitigados: 7.1.5

- La destrucción de tarjetas dañadas deberá realizarse semanalmente y en presencia de un representante de Auditoría o Legal, y de Seguridad de Información (dos como mínimo), y deberá contar con un Acta de Destrucción donde se constate la presencia de los veedores y el número de tarjetas a destruir. El modelo de Acta de Destrucción se muestra en la figura 5.6:

ACTA DE DESTRUCCIÓN DE TARJETAS
Fecha: ___de_____del 200___

Participantes	
Número de Tarjeta	
Motivo de destrucción	

Firman en señal de conformidad, a las ____ horas:

_____ Seguridad de Información

_____ Auditoría Interna/ Asesoría Legal

Figura 5.6. Acta de Destrucción de Tarjetas

Riesgos mitigados: 7.1.5

5.6 De la operación

5.6.1 Procesamiento de la información

- Todo PIN ingresado por un tarjetahabiente en un ATM se debe procesar en los equipos HSM y en ningún otro equipo.

  Riesgos mitigados: 8.1.1

- Los PINs no aparecerán nunca almacenados en texto claro en ninguna base de datos, archivo o sistema. Su almacenamiento deberá ser exclusivamente en valor encriptado. Dichos valores deben ser generados sólo a partir de los HSM.

  Riesgos mitigados: 8.1.2

5.6.2 Flujo de instalación de llaves desde los HSM a los ATM

La instalación de las llaves criptográficas en los ATM, bajo el esquema de llaves públicas ya no será realizada por dos custodios en el lugar de ubicación de cada cajero automático.

La instalación de las llaves en el cajero seguirá el siguiente flujo:

1. El HSM genera un par de llaves, una pública Pub(H) y una privada Pri(H).
2. La llave pública Pub(H) es enviada por el Switch Central al ATM.
3. El ATM genera un par de llaves, una pública Pub(A) y una privada Pri(A).
4. El ATM encripta la llave pública Pub(A) bajo la llave pública Pub(H).
5. El HSM genera una TMK y la encripta bajo la llave pública Pub(A) – para resguardar la confidencialidad de la TMK – transmitida por el ATM y firma dicho mensaje bajo su llave privada Pri(H) – para asegurar el no repudio y la autenticación del HSM.
6. El ATM verifica la firma del HSM y desencripta la TMK con su llave privada Pri(A).
7. El HSM genera la TPK, la encripta bajo la TMK y la envía al ATM.
8. El ATM inicia sus operaciones con dicha TPK.

5.6.3 Transacciones en ATMs del Banco de la Nación

5.6.3.1 Transacciones On-US – Rol Emisor

1. La información ingresada en el cajero es encriptada bajo la llave TPK.
2. En el switch central se desencripta la información con la TPK y se determina que es una transacción On-US.
3. Se resuelve la transacción en el computador central y devuelve la respuesta al ATM.

5.6.3.2 Transacciones Domésticas – Rol Adquirente

1. La información ingresada en el cajero es encriptada bajo la llave TPK.
2. En el switch central se desencripta la información con la TPK y se determina que es una transacción doméstica.
3. Firma la información con la llave pública Pub(ZMK_{BNV}) de Visanet Perú y la envía a Visanet Perú.
4. Visanet Perú desencripta la información con su llave privada Pri(ZMK_{BNV}) con el Banco de la Nación.
5. Determina a la entidad doméstica A a la cual pertenece la transacción.
6. Firma la transacción con la llave pública Pub(ZMK_{A}) de la entidad A y se la envía.
7. La entidad A desencripta la información con su llave privada Pri(ZMK_{A}) y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública Pub(ZMK_{AV}) a Visanet Perú.
9. Visanet Perú desencripta la información con su llave privada Pri(ZMK_{AV}) con la entidad A.
10. Determina al Banco de la Nación como adquirente de la transacción.
11. Firma la transacción con la llave pública Pub(ZMK_{BN}) del Banco y se la envía.

12. El Banco desencripta la información con su llave privada Pri(ZMK_{BN}) y responde al ATM encriptando la información bajo la TPK.

5.6.3.3 Transacciones Internacionales – Rol Adquirente

1. La información ingresada en el cajero es encriptada bajo la llave TPK.
2. En el switch central se desencripta la información con la TPK y se determina que es una transacción internacional.
3. Firma la información con la llave pública Pub(ZMK_{BNV}) de Visa y se la envía.
4. Visa desencripta la información con su llave privada Pri(ZMK_{BNV}) con el Banco de la Nación.
5. Determina al emisor E a la cual pertenece la transacción.
6. Firma la transacción con la llave pública Pub(ZMK_{E}) del emisor E y se la envía.
7. El emisor E desencripta la información con su llave privada Pri(ZMK_{E}) y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública Pub(ZMK_{EV}) a Visa.
9. Visa desencripta la información con su llave privada Pri(ZMK_{EV}) con el emisor E.
10. Determina al Banco de la Nación como adquirente de la transacción.
11. Firma la transacción con la llave pública Pub(ZMK_{BN}) del Banco y se la envía.
12. El Banco desencripta la información con su llave privada Pri(ZMK_{BN}) y responde al ATM encriptando la información bajo la TPK.

5.6.4 Transacciones en ATMs de otros bancos

5.6.4.1 Transacciones Domésticas – Rol Emisor

1. La información ingresada en el cajero de otro banco X es encriptada bajo la llave TPK.
2. En el switch central se desencripta la información con la TPK y se determina que es una transacción doméstica.
3. Firma la información con la llave pública Pub(ZMK_{XV}) de Visanet Perú y la envía a Visanet Perú.
4. Visanet Perú desencripta la información con su llave privada Pri(ZMK_{XV}) con el banco X.
5. Determina que la entidad emisora es el Banco de la Nación.
6. Firma la transacción con la llave pública Pub(ZMK_{BN}) del Banco de la Nación y se la envía.
7. El Banco de la Nación desencripta la información con su llave privada Pri(ZMK_{BN}) y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública Pub(ZMK_{BNV}) a Visanet Perú.
9. Visanet Perú desencripta la información con su llave privada Pri(ZMK_{BNV}) con el Banco de la Nación.
10. Determina al Banco X como adquirente de la transacción.
11. Firma la transacción con la llave pública Pub(ZMK_{X}) del Banco X y se la envía.
12. El Banco X desencripta la información con su llave privada Pri(ZMK_{X}) y responde al ATM encriptando la información bajo la TPK.

5.6.4.2 Transacciones Internacionales – Rol Emisor

1. La información ingresada en el cajero del Banco Y es encriptada bajo la llave TPK.

2. En el switch central se desencripta la información con la TPK y se determina que es una transacción internacional.
3. Firma la información con la llave pública Pub(ZMK_{YV}) de Visa y se la envía.
4. Visa desencripta la información con su llave privada Pri(ZMK_{YV}) con el Banco Y.
5. Determina que la entidad emisora es el Banco de la Nación.
6. Firma la transacción con la llave pública Pub(ZMK_{BN}) del Banco de la Nación y se la envía.
7. El Banco de la Nación desencripta la información con su llave privada Pri(ZMK_{BN}) y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública Pub(ZMK_{BNV}) a Visa.
9. Visa desencripta la información con su llave privada Pri(ZMK_{BNV}) con el Banco de la Nación.
10. Determina al Banco Y como adquirente de la transacción.
11. Firma la transacción con la llave pública Pub(ZMK_{YN}) del Banco Y y se la envía.
12. El Banco Y desencripta la información con su llave privada Pri(ZMK_{YN}) y responde al ATM encriptando la información bajo la TPK.

5.6.5 Flujo de aceptación de operaciones de una tarjeta chip en un ATM

Paso 1: Comenzar una transacción

Para comenzar una transacción, la tarjeta chip es insertada dentro del ATM. El chip en la tarjeta se conecta con los contactos en el ATM para que puedan comunicarse uno con el otro. La tarjeta debe permanecer en éste hasta que la transacción esté completada.

Paso 2: Selección de la aplicación

El ATM determina cuales aplicaciones son soportadas tanto por él como por la tarjeta. Si la tarjeta y el ATM no tienen aplicaciones en común, la transacción es terminada. Si la tarjeta y el ATM tienen una aplicación en común, esa aplicación es usada. Si la tarjeta y el ATM tienen más de una aplicación en común, el ATM muestra una lista de aplicaciones para la selección del tarjetahabiente. Una vez que la aplicación es seleccionada, la tarjeta envía información al ATM para ser usada durante la transacción.

Paso 3: Verificación del tarjetahabiente

La tarjeta y el ATM trabajan conjuntamente para determinar el método de verificación apropiado para la transacción (tanto la firma, PIN en línea, verificación del tarjetahabiente). Si el método de verificación del tarjetahabiente es PIN fuera de línea, el terminal solicita al tarjetahabiente el ingreso de su PIN. El PIN ingresado del tarjetahabiente es comparado con el PIN almacenado en el chip por el emisor durante el proceso de personalización de la tarjeta. Los métodos de verificación en línea son implementados de manera similar a la banda magnética.

El Banco de la Nación debe implementar todas las modalidades disponibles en sus cajeros automáticos. La verificación del PIN fuera de línea debe realizar como primera medida antes de enviar los datos de la transacción al switch central. En casos de contingencia, esta verificación debe realizarse cuando exista conexión con el computador central pero no exista respuesta del Switch Stratus o del HSM.

Paso 4: Transacciones en línea

Cuando la tarjeta y el ATM deciden enviar una transacción en línea y la tarjeta soporta la facilidad de autenticación de tarjeta en línea, el chip genera un criptograma ARQC resultado de la encripción de los datos de la tarjeta, el ATM, y la transacción bajo la TPK. El criptograma es único por cada transacción. El chip de la tarjeta envía el criptograma y los datos al terminal.

El terminal envía el criptograma, y los elementos de datos originales usados por el chip para crear el criptograma, al adquirente. El adquirente formatea estos datos en el mensaje de autorización y los envía al emisor a través de la red en línea.

Paso 5: Procesamiento del emisor

El emisor valida el criptograma y usa los resultados de la autenticación de la tarjeta en línea en su decisión de autorización. El emisor puede también usar los resultados de la administración de riesgos fuera de línea, como el PIN fuera de línea y la autenticación de datos fuera de línea, para determinar la respuesta de autorización.

Paso 6: Respuesta del emisor

Para proteger la respuesta de autorización del emisor y asegurar que la respuesta venga de un emisor válido, el emisor tiene la habilidad de enviar un criptograma para la autenticación del emisor en línea en la respuesta. Este criptograma es llamado Criptograma de Respuesta de Autorización.

El emisor también tiene la opción de enviar actualizaciones post emisión para la tarjeta en la respuesta. Estas actualizaciones permiten al emisor cambiar información en la tarjeta después de que ésta ha sido emitida. Antes de aplicar las actualizaciones Post emisión, la tarjeta asegura que se está comunicando con un emisor válido.

Cuando la tarjeta recibe la respuesta, ésta aplica la actualización post emisión (si está presente) después de asegurar de que las actualizaciones provienen del emisor correcto. El código de respuesta de autorización es usado para determinar si la transacción es aprobada o declinada.

Paso 7: Compensación y Pago

Ya sea para transacciones aprobadas en línea o fuera de línea, la tarjeta genera un criptograma final llamado Certificado de Transacción. Este criptograma y sus elementos de datos soportados representan una pista de auditoría. Las pistas de auditoría proveen evidencia de las actividades realizadas por la tarjeta y el terminal de punto de la transacción. Esta información es incluida con el mensaje de compensación y pueden ser usados durante un proceso de disputa.

Beneficios

- Disminución del costo de inicialización de los cajeros automáticos.
- Reducción del riesgo de compromiso por conocimiento de los componentes de las claves.
- Minimizar el uso de personal para labores de operación con claves.
- Protección de las claves simétricas secretas.

Capítulo 6: Conclusiones y trabajos futuros

En esta sección se presentan las conclusiones del trabajo de investigación, así como trabajos futuros que se pueden desarrollar a partir del mismo.

6.1 Conclusiones

- La seguridad de información se ha convertido en un elemento básico que determina el éxito o fracaso de las empresas, al mantener o no la privacidad e integridad de la información de sus clientes.
- Las llaves criptográficas tienen como función principal resguardar la confidencialidad de la información personal y/o privada de personas o instituciones.
- El éxito de la implementación de cualquier infraestructura criptográfica en una institución se determina según el nivel adecuado o no de administración de las llaves criptográficas, equipos y personas relacionadas a los procesos de generación, almacenamiento, carga, verificación, respaldo y eliminación de dichas llaves criptográficas.
- Una correcta implementación de los controles de seguridad de información señalados en el capítulo 5, reducen el alto nivel de riesgo detectado en el capítulo de Evaluación de Riesgos.
- La eficacia de los algoritmos asimétricos en comparación con los algoritmos simétricos hace que sea necesario, para aquellas instituciones que desean mantener una imagen de confiabilidad ante sus clientes, que dichas instituciones inicien su adecuación a medidas de seguridad más fuertes, tratando de aminorar el impacto de los cambios hacia los clientes.
- El uso de hardware para la implementación de controles seguridad de información, tales como equipos HSM y tecnología de circuitos integrados, hace que aumente el nivel de confianza ante posibles fallos o brechas.
- Procedimientos documentados y validados apropiadamente hace que los controles sean más fuertes.

6.2 Trabajos Futuros

- Se debe realizar un trabajo de migración del Banco de la Nación de todos los canales de atención para su validación en los equipos HSM, de manera que la implementación de los controles descritos permitan la implementación de mayores controles de seguridad de información en aquellos canales no estudiados en este trabajo.
- Dado que la tecnología chip se está diseminando a través del mundo, es necesario que los comercios, adquirentes y emisores cambien los equipos que no cuenten con funciones EMV, para su adecuación a la tendencia mundial.

Capítulo 7: Glosario de Términos

- ANSI : American National Standards Institute
- ATM : Automatic Teller Machine
- ATR : Answer To Reset
- CVC : Card Verification Code
- CVV : Card Verification Value
- DES : Data Encryption Standard
- DEA : Data Encryption Algorithm
- DUKPT : Derived Unique Key Per Transaction
- EDI : Electronic Data Interchange
- EEPROM : Electrically-Erasable Programmable Read-Only Memory
- EMV : Europay, MasterCard and Visa
- EMVCo : EMV Company
- FIPS : Federal Information Processing Standards
- HSM : Host Security Module
- ICC : Integrated Circuit Card
- IEC : International Electrotechnical Commission
- INDECOPI : Instituto Nacional de Defensa de la Competencia y Propiedad Intelectual
- ISO : International Organization for Standardization
- NIST : National Institute of Standards and Technology
- NTP : Norma Técnica Peruana
- NSA : National Security Agency
- PCM : Presidencia del Consejo de Ministros
- PIN : Personal Identification Number
- PKI : Public Key Infrastructure
- POS : Point of Sale
- PVV : PIN Verification Value

- RAM : Random Access Memory
- ROM : Read Only Memory
- RSA : Rivest, Shamir y Adleman
- SBS : Superintendencia de Banca, Seguros y AFP
- SGSI : Sistema de Gestión de Seguridad de Información
- SSAD : Signed Static Application Data
- TDEA : Triple DEA
- TI : Tecnologías de Información
- TRSM : Tamper-Resistant Security Module
- XOR : Exclusive OR

Capítulo 8: Referencias Bibliográficas

[Acev+04] Acevedo Zamorano Freedy y Vargas Malebrán Verónica, Seguridad en el Comercio Electrónico, Universidad de Chile, Tesis para optar al título de Ingeniero en Información y Control de Gestión, 2004, Chile

[BN08] Banco de la Nación, Home Banking, http://www.bn.com.pe/NuestroBanco/acercadelbn.asp, Acerca del Banco, 2008

[BNCC07] Banco de la Nación – Comunicación Corporativa, 31-05-2007, http://www.bn.com.pe/Modulos/noticias_detalle31052007.asp, Lima-Perú

[BNSI07] Banco de la Nación-División Seguridad de Información, Diciembre 2008, Lima-Perú

[D'Andrea98] D'Andrea Giovanni Diliana, http://www.monografias.com/trabajos/franquicia/franquicia.shtml, 1998, San Joaquín de Turmero

[ECBS03] European Committee for Banking Standards ECBS, Guidelines on Algorithms Usage and Key Management, 2003, Bruselas.

[EMVCo03] EMV Issuer and Application Security Guidelines, Versión 1.2, Julio 2003

[Güimack07] Güimack Peña Janet, Historia de la Criptografía, http://jagupe.wordpress.com/category/criptografia/, 14 Agosto 2007

[INDECOPI07] Instituto Nacional de Defensa del Consumidor y de la Propiedad Intelectual INDECOPI, Norma Técnica Peruana NTP ISO/IEC 17799: 2007 EDI Tecnologías de Información. Código de Buenas Prácticas para la Gestión de la Seguridad de Información, 2007, Segunda Edición, Lima-Perú.

[INEI02] Instituto Nacional de Estadística e Informática INEI, Guía para la elaboración del Plan de Seguridad de la Información, 2002, Lima-Perú.

[Jones08A] Jones Don, Introducción a la Administración de Seguridad, Real Time Publishers y Computer Associates, http://www.ca-smx.com/la/papers/iam_ebook_capítulo_1.pdf, 2008.

[Jones08B] Jones Don, Continuidad del Servicio, Real Time Publishers y Computer Associates, http://www.ca-smx.com/la/papers/iam_ebook_capítulo_9.pdf, 2008.

[Lucena99] Lucena López, Manuel José, Criptografía y Seguridad en Computadores, Escuela politécnica Superior – Universidad de Jaén, 1999

[MCWW08] MasterCard Worldwide, Interchange http://www.mastercard.com/us/company/en/newsroom/interchange_payment_industry.html, Home Banking, 2008

[Medaglia01] Medaglia Diego, Tarjetas Inteligentes, Licenciatura de Análisis de Sistemas de Información, Universidad ORT - Facultad de Ingeniería, http://www.monografias.com/trabajos16/tarjetas-inteligentes/tarjetas-inteligentes.shtml, Uruguay, 2001

[Ponce04] Ponce José, Firma Digital, Common Perú, Lima-Perú

[Thales04] Thales e-Security Limited, Host Security Module 8000 Console Reference Manual, Thales e-Security Limited, 2004

[Thales05] Thales e-Security Limited, El Ambiente Bancario, 2005

[Thales07] Thales e-Security Limited, Host Security Module 8000, http://www.thales-esecurity.com/productsservices/Documents/11653-HSM8000-v2.pdf, 2007

[Torres06] Torres Márquez Joaquín, Nuevo marco de autenticación para tarjetas inteligentes en red - Aplicación al pago electrónico en entornos inalámbricos, Universidad Carlos III de Madrid, Tesis doctoral (2006), Leganés - España.

[Visa02] Visa International Región América Latina y el Caribe, Introducción a la Criptografía y Seguridad del PIN - Administración de Riesgo, Enero del 2002, Florida - USA

[Visa06A] Mejores Prácticas de Administración de Riesgo para Fraude en ATM - Versión 1.6, Oficina de Administración de Riesgo Región América Latina y el Caribe, Junio 2006

[Visa06B] Programa de la Seguridad del PIN - Criptografía Asimétrica - Seguridad del PIN y Administración de Llaves, Lima - Perú, 2006

[Visa07] Unidad de Administración de Riesgo, Skimming, Visa Latinoamérica, Boletín Informativo para Emisores y Adquirentes (2007), Florida – Estados Unidos.

[Visa99] Visa International, Primer: EMV, VIS, Acceptance and Interoperability Versión 2.0; Acceptance Channels – External Standards, https://www.lac.visaonline.com/la_prodmktg/chip_cards/Implementation/PRIMER-EMV-VIS-2-0-INSITE.pdf, Octubre 1999

[Wikipedia08a] Wikipedia, Seguridad de la Información, http://es.wikipedia.org/wiki/Seguridad_de_Informaci%C3%B3n, 29-02-2008

[Wikipedia08b] Wikipedia, Franquicias, http://es.wikipedia.org/wiki/Contrato_de_Franquicia#Historia, 03-03-2008