Índice

Capítulo 1

Introducción

Actualmente, existe la cultura de la utilización de las tarjetas con banda magnética, con las cuales se llevan a cabo un gran número de operaciones y transaciones de diversa índole.

Una de las caracteristicas más importantes que se requieren en un programa de tarjetas, es la seguridad de la información y de las transacciones que se realizan con ellas.

De acuerdo con lo anterior, con otra dinámica y en crecimiento cada vez más acelerado, los programas de tarjetas se están diseñando con las llamadas tarjetas inteligentes.

Aún cuando es marginal el uso de las tarjetas inteligentes en ambiente de multiaplicaciones, las tendencias, tanto de los organismos de estandarización y grupos de emisores, es hacia la explotación y madurez de los ambientes de tarjetas de multiaplicaciones de diversos proveedores.

La migración, adopción o ampliación de un programa de tarjetas inteligentes, requiere de un cambio cultural, organizativo y tecnológico, adicional a los grandes beneficios que conlleva la seguridad que proporcionan las tarjetas inteligentes, está el cambio de paradigma de la utilización de diversas tarjetas de banda mágnetica por una sola tarjeta inteligente, trayendo consigo importantes mejoras en la economía y en la eficacia de los procesos involucrados en la operación de las tarjetas.

Así también, otra diferencia de importancia entre los ambientes de operación entre estos dos tipos de tarjetas, es la real posibilidad de realizar la mayoría de las transacciones sin que las terminales de lectura de las tarjetas tengan que estar conectadas a los servidores de los operadores de los programas de tarjetas, trayendo consigo importantes economías por concepto de conexión remota y administración en línea para el manejo de las transacciones electrónicas.

En este contexto, las herramientas para la administración de estos programas, también están migrando hacia diferentes esquemas, de acuerdo a las necesidades que plantean las etapas por las que una tarjeta inteligente atraviesa, desde su diseño, pasando por su utilización, hasta la terminación de su vida útil.

Aunque en esencia los procesos en los que las tarjetas de banda magnética e inteligentes participan, tanto los de su fabricación como los de la operación, tienen la misma denominación, el detalle y forma de llevarlos a cabo son completamente diferentes.

En este entendido, esta tesis aborda los procesos que están en el estado del arte para la gestión de una tarjeta inteligente.

A saber, según Fabio A. González del Departamento de Ingeniería de Sistemas e Industrial de la Universidad Nacional de Colombia [W12], el estado del arte

> "de un trabajo, resume y organiza los resultados de investigación reciente en una forma novedosa que integra y agrega claridad al trabajo en un campo específico.",

con las siguientes características:

- Asume un conocimiento general del tema
- Enfatiza la clasificación de la literatura existente
- Evalúa las principales tendencias
- Desarrolla una perspectiva del tema
- Establece un tiempo de la investigación
- Señala los ámbitos y el alcance

En este contexto, se trata de vincular el estado del arte de dos áreas del conocimiento; por un lado, referirse a los resultados de los trabajos realizados por las diferentes industrias y organismos internacionales de estandarización que convergen en las tarjetas inteligentes y por otra emplear las mejores prácticas, técnicas y herramientas disponibles en la actualidad para la adopción y puesta en operación de un sistema de información al servicio de la gestión de las tarjetas inteligentes.

Actualmente hay un importante número de resultados concretos de estandarización, encabezados por organismos como ISO (International Standard Organization), IEC (International Electrotechnical Commite), ITU (International Telecommunications Union), que han establecido las bases para alcanzar la normalización y estandarización de características generales y de otros organismos especializados como Global Platform y EMV (Europay Master Visa) con contribuciones de especificaciones y normas para diferentes sectores especializados, este trabajo emplea el estado actual de las especificaciones publicadas por ellos.

Embebidas en nuestro segundo componente, están las etapas de la conceptualización, modelado e implementación del SGTI.

Partiendo del entendimiento que se tiene de un sistema de información, el cual según el diccionario Webster [W13] establece que es un:

- "Grupo de elementos independientes, pero interrelacionados que comprende un conjunto unificado,
- Instrumento que combina objetos que interactúan entre sí, diseñado para funcionar como una entidad coherente
- Conjunto de métodos
- Procedimiento o proceso para la obtención de un objetivo
- Una estructura organizada para alcanzar una visión"

A saber, los elementos independientes a integrar y correlacionar para obtener el sistema de información, son las reglas de negocios, los perfiles de las tarjetas, las entidades empresariales involucradas y los roles que ejecutan, el personal participante, la infraestructura de la industria y de los usuarios, el software base, el hardware, las aplicaciones y la seguridad de la información.

Por la complejidad de los procesos, el perfil heterogéneo de los participantes, las áreas de conocimiento especializado y diversidad de ambientes de operación de las tarjetas, es necesario adoptar un enfoque de Ingeniería de sistemas para su conceptualización, modelado e implementación.

De acuerdo con Pressman [3], la Ingeniería de software ocurre como consecuencia de un proceso llamado Ingeniería de sistemas. En lugar de concentrase sólo en el software, esta disciplina se centra en todos los elementos que lo componen, mientras analiza, diseña y organiza aquellos componentes de un sistema que pueden ser un producto, un servicio o una tecnología para la transformación o control de información.

Siguiendo con Pressman [3], el proceso de Ingeniería de sistemas asume distintas formas, según el dominio de la aplicación en que se utilice. La Ingeniería de procesos de negocios se aplica cuando el contexto del trabajo se enfoca en una organización. Cuando se enfoca en la elaboración de un producto, al proceso se le conoce como Ingeniería del producto.

De acuerdo con Pressman [3], la meta de la Ingeniería de procesos de negocios, es definir arquitecturas que permitan que un negocio utilice información de manera efectiva.

En términos de lo anterior para este trabajo se adopta un enfoque de Ingeniería de sistemas, las especificaciones de las arquitecturas que conforman el sistema de información se desarrollan de acuerdo al marco de arquitectura empresarial de información.

La gestión de las tarjetas inteligentes es la funcionalidad principal del sistema de información, tema de este trabajo.

La fabricación de una tarjeta inteligente, de acuerdo a especificaciones, estándares, normas, requerimientos del cliente, necesidades de los usuarios, conlleva la planeación, diseño, ejecución y mejora de un conjunto de procesos productivos.

Por otro lado, para que tenga sentido estudiar un sistema de gestión de tarjetas inteligentes (SGTI), es importante que su diseño y operación se encuentre en el dominio de las tarjetas multiaplicativas.

Una tarjeta multiaplicativa, es aquella que puede alojar de manera simultánea más de una aplicación, pudiendo ser estas primarias o de propósito específico, con la característica de que estas aplicaciones no son estáticas en el tiempo.

De manera general, podemos decir que nos referimos a la gestión de la sistematización y automatización de procesos de: fabricación, ensamble, diseño electrónico, personalización gráfica y eléctrica, desarrollo y mantenimiento de software, implementación de la seguridad de la información y configuración de infraestructura tecnológica.

En el contexto de las tarjetas inteligentes, la interrelación entre diversas disciplinas, el mercado y las industrias asociadas ha impulsado el establecimiento de referentes, normas y estándares que faciliten la interoperabilidad, favorezcan la compatibilidad y se fomenten los sistemas abiertos.

En este tenor, un sistema de gestión de tarjetas inteligentes, es en esencia una herramienta que atiende el ciclo de vida de las tarjetas inteligentes y de las aplicaciones que corren en ella, ciclo que se define desde la fabricación del circuito integrado, hasta la finalización en el uso de la tarjeta.

Cada una de estas etapas del ciclo tiene un vínculo directo con los procesos de fabricación en planta, los procesos de tecnología de la información, así como los del registro de los eventos que ocurren durante la vida útil de la tarjeta en correlación con los titulares, emisores y socios de negocio que están involucrados en su uso y manejo.

La existencia de estos procesos, involucra la participación de diversas entidades empresariales que son las que activan y realizan los eventos.

Por tanto, en atención a la definición de estado del arte adoptado y a sus características, el desarrollo de este trabajo toma en cuenta lo siguiente:

Características	Actividades a desarrollar
• Asume un conocimiento general del tema	Se expondrán los principales conceptos asociados a las tarjetas inteligentes, arquitecturas empresariales de información, procesos de gestión de tarjetas inteligentes y gestión de llaves criptográficas
• Enfatiza la clasificación de la literatura existente	Se presentarán los referentes principales de la literatura disponible en la actualidad, cuyas fuentes principales son la industria, los organismos de estandarización, los grupos emisores especializados y material académico

Características	Actividades a desarrollar
• Evalúa las principales tendencias	Se revisarán las actuales tendencias, obteniendo su comparación y evaluación
• Desarrolla una perspectiva del tema	Se obtendrá y se presentará un enfoque y visión del tema a partir de los estados del arte de los componentes: tarjetas inteligentes, procesos de gestión de tarjetas, arquitecturas empresariales de información y estándares de la Industria de las tecnologías de la información
• Establece un tiempo de la investigación	Es el tiempo dedicado desde la identificación de las diversas fuentes, su análisis e integración, hasta la redacción del presente trabajo.
• Señala los ámbitos y alcance	El ámbito y alcance es para el ambiente multiaplicativo de tarjetas inteligentes, se excluyen de los conceptos de tarjetas inteligentes los relativos a: las tarjetas telefónicas, los procesos de personalización gráfica, la descripción de los materiales de fabricación, el ciclo de desarrollo de las aplicaciones a instalar en las tarjetas, el nivel de conformidad de la seguridad de los componentes de la plataforma y los procesos de transporte y ceremonia de llaves.

1.1 Definición del problema

El ciclo de vida de las tarjetas inteligentes es un conjunto de eventos que ocurren a través del tiempo, los cuales incluyen los procesos productivos para su fabricación, el desarrollo de aplicaciones a ser incorporadas en ellas, la implementación de los esquemas de seguridad y la activación para su empleo.

En estas actividades se ven involucradas un conjunto de entidades empresariales con roles definidos, las cuales tienen dependencia entre sí para lograr su correcta operación.

La gestión de las tarjetas inteligentes cobra mayor importancia, por la complejidad de los procesos y la concurrencia de varias entidades empresariales en la medida que las aplicaciones que se instalan crecen en número y funcionalidad.

El ambiente con varias aplicaciones que se instalan en una misma tarjeta inteligente, se conoce como multiaplicaciones, las cuales también en algunos casos pueden ser multiproveedores.

Este entorno requiere de un sistema de gestión, totalmente articulado, con definición clara de los roles y los tiempos de las actividades a realizar.

El ambiente de operación de este sistema puede ser centralizado o descentralizado, según el diseño del propio Programa de tarjetas al que corresponde.

Intrínsecamente, el potencial de las tarjetas inteligentes es la movilidad de los datos contenidos en ellas que permite ejecutar transacciones en cualquier lugar y momento, con la premisa de que exista la infraestructura necesaria, la cual debe de ocurrir en un ambiente de seguridad, confidencialidad y garantía para los usuarios y dueños de las tarjetas.

En este contexto se requiere disponer de un sistema de información para la gestión de las tarjetas inteligentes que permita incorporar todas las etapas del ciclo de vida de las tarjetas y de las aplicaciones instaladas en ellas, en un ambiente de integridad y seguridad de datos, que brinde el potencial de emplear el estado del arte de cada uno de los componentes de la solución.

1.2 Antecedentes

A partir de las tarjetas de banda magnética, la evolución de las tarjetas inteligentes ha permitido además de un incremento notable en su capacidad de almacenamiento, prestaciones en materia de seguridad de la información y versatilidad en el tipo y número de aplicaciones a ser instaladas y ejecutadas.

Además de la diferencia entre las características de cada tecnología, el referente principal para la comparación entre ambos tipos de tarjetas es el del ciclo de vida de las tarjetas. Este atributo es el que hace la principal diferencia para que un sistema de gestión permita un seguimiento puntual de cada uno de los eventos y operaciones de las tarjetas, asociados con los operadores y usuarios de las mismas.

El salto evolutivo de los sistemas de gestión de tarjetas de banda magnética hacia los de tarjetas inteligentes, cubren la brecha desde el nacimiento de la misma tarjeta, pasando por la forma de operación necesariamente centralizada a una amplia gama de combinaciones de configuraciones y modos de operación y la posibilidad de carga y descarga de aplicaciones en etapas de postemisión.
En esta medida la gestión de las tarjetas y sus aplicaciones demandan procesos y sistemas para poder proporcionar mejores servicios a los usuarios de las mismas, así como a las entidades empresariales involucradas en la cadena de servicio.

1.3 Objetivos

1.3.1 Objetivo general

Desarrollar una metodología que permita construir la especificación de un sistema de información para la gestión de tarjetas inteligentes (SGTI), de acuerdo al estado del arte que presente la industria de las mismas.

1.3.2 Objetivos particulares

- Integrar las principales características de las tarjetas inteligentes
- Definir el modelo para el desarrollo de las especificaciones funcionales
- Integrar las especificaciones para la gestión de las tarjetas inteligentes
- Integrar las especificaciones para la implementación del SGTI
- Desarrollar un modelo para la implementación y gobierno del SGTI

1.4 Metodología

Realizar una investigación exploratoria sobre el tema de las tarjetas inteligentes, reuniendo y analizando el material actual que se ha publicado en libros, artículos e información producida por la industria.

Seleccionar los aspectos más relevantes, que permitan un entendimiento claro y amplio de la tecnología de las tarjetas inteligentes.

Realizar el estudio y seleccionar los temas que se asocian con los aspectos de seguridad de la información en tarjetas inteligentes.

Investigar en diferentes materiales disponibles los procesos de manufactura de las tarjetas inteligentes.

Investigar y seleccionar los marcos de referencia para desarrollar la conceptualización, modelado e implementación de un SGTI.

Investigar, analizar y seleccionar las mejores prácticas de las tecnologías de la información aplicables a este trabajo.

Integrar la información seleccionada y desarrollar el modelo propuesto para la implementación y gobierno de un SGTI.

1.5 Alcance

La propuesta de la metodología para la implementación y gobierno de un SGTI, abarca los procesos de preemisión, emisión y postemisión de las tarjetas inteligentes, no contemplando:

- Las especificaciones de las tarjetas telefónicas
- La descripción de los procesos de personalización gráfica

- La descripción de los procesos relativos a los materiales de las tarjetas
- Las especificaciones de los procesos de la cadena de valor y de soporte de:
    - Logística de salida
    - Mercadotecnia y ventas
    - Servicio
    - Adquisiciones
    - Administración de recursos humanos
    - Infraestructura organizacional
- La especificación de los procesos de transporte y ceremonia de llaves
- El ciclo de desarrollo de las aplicaciones de las tarjetas
- La descripción de los procesos de conformidad de la seguridad de los componentes integrados EAL e ITSEC.

1.6 Estructura del documento

Al inicio de cada apartado se da un bosquejo general del tema a tratar, para los casos en que se requiera se refiere a algún apartado anterior que esté relacionado, así mismo al final del apartado se concluye con el impacto del mismo en la funcionalidad del sistema de gestión de tarjetas inteligentes.

En el Capítulo 1, se describen el marco general para el desarrollo de esta tesis, tales como antecedentes, objetivos y metodología de desarrollo de la misma.

El Capítulo 2, está dedicado a los conceptos básicos necesarios de las tarjetas inteligentes a ser incorporados en la especificación del SGTI, tales como los diferentes tipos de tarjetas inteligentes y sus componentes, características de los sistemas operativos, fases del ciclo de vida de las tarjetas y las aplicaciones, algoritmos criptográficos para la seguridad de la información en las tarjetas, los estándares de la industria que aplican y la arquitectura de la tarjeta.

En el Capítulo 3, se describe el marco de referencia bajo el cual se estudia el SGTI, los diversos componentes que lo integran y los sistemas de información que tienen interfaz con él.

En el Capítulo 4, con base en el marco de referencia del desarrollo del sistema se integran las especificaciones de las diversas arquitecturas que lo componen, el plan de migración e implementación y el gobierno del SGTI.

Finalmente en el Capítulo 5, se describen los resultados, impacto y conclusiones de este trabajo.

Capítulo 2

Conceptos básicos de las tarjetas inteligentes

2.1 Evolución de las tarjetas inteligentes

Este capítulo refiere los antecedentes y los procesos de evolución de las tarjetas inteligentes, mencionado los momentos importantes en cuanto a su desarrollo o aspectos que han sido relevantes para su consolidación.

De acuerdo a los estándares ISO/IEC 7810, 7811 y 7816 [W15], y a lo que plantea el Government Smart Card Handbook [R2], una tarjeta inteligente es una tarjeta fabricada de la combinación de diversos materiales principalmente de Polivinilo de cloruro (PVC) y policarbonato, cuyas dimensiones son 85.6 mm X 53.97 mm, que contiene uno o más circuitos integrados (CI) y que también puede emplear uno o más equipos de diferente tecnología para la lectura de banda magnética, código de barras (lineales o bidimensionales), de contacto, radio frecuencia sin contacto, información biométrica, cifrado y autenticación o identificación con fotografía.

En la memoria del chip se almacenan los datos y se puede acceder a él para completar las solicitudes de procesamiento. La memoria del chip del microprocesador también contiene el sistema operativo (SO), software de comunicaciones, y también puede contener algoritmos de cifrado.

Cuando se utiliza en conjunto con las aplicaciones adecuadas, las tarjetas inteligentes pueden proporcionar seguridad y la capacidad de grabar, almacenar y actualizar datos. Cuando se implementa correctamente, pueden proporcionar la interoperabilidad entre servicios u organismos, y permiten las aplicaciones o usos múltiples con una sola tarjeta.

Como herramientas de pago, las tarjetas inteligentes pueden servir de crédito, débito o de valor almacenado de pago y/o instrumentos de pago simbólico y proporcionar la capacidad para acceder a las cuentas financieras y la transferencia de fondos entre cuentas.

La mejora del acceso seguro a las instalaciones, con el uso de tecnologías como la biometría e infraestructura de llave pública (PKI por sus siglas en ingles) mejora la seguridad de la verificación de identidad en el acceso físico y lógico. PKI utiliza las llaves públicas y privadas para la firma digital, el cifrado y descifrado.

La biometría utiliza las características físicas de las personas (por ejemplo, huellas dactilares, geometría de la mano, escaneo del iris y de voz o de reconocimiento facial) para autenticar la identidad de un individuo. PKI y/o la biometría se puede usar para identificar con más precisión a un individuo.

Tal como lo señala Wolfgang Ranki [17], la proliferación de las tarjetas de plástico se inició en los Estados Unidos de Norte América en la década de 1950. El bajo precio del material sintético PVC hizo posible la producción de materiales sólidos, las tarjetas de plástico duradero eran mucho más adecuadas para el uso

diario que las tarjetas de papel y cartón, que no podían soportar adecuadamente los esfuerzos mecánicos y los efectos climáticos.

La primera tarjeta de pago de plástico para uso general fue emitida por Diners Club en 1950.

Información general, como el nombre del emisor de la tarjeta, fue impreso en la superficie, mientras que los elementos de los datos personales, tales como el nombre del titular y el número de tarjeta, fueron grabados de manera interna. A muchas tarjetas también se les agrego un panel de firma en que el titular de la tarjeta puede firmar como referencia. En esta primera generación de tarjetas, la seguridad fue proporcionada por las características gráficas.

La primera mejora consistió en una banda magnética en el reverso de la tarjeta, lo que permitió que los datos se almacenaran en la tarjeta en forma legible para ser procesados mediante una máquina, como un complemento a la información visual.

Sin embargo, la tecnología de banda magnética, tiene una debilidad fundamental, que los datos almacenados en la banda pueden ser leídos, borrados y reescritos por cualquier persona con acceso a cierto tipo de equipo.

Por lo tanto, este tipo de tarjetas no son recomendables para el almacenamiento de datos confidenciales. Técnicas adicionales deben de ser utilizadas para garantizar la confidencialidad de los datos y evitar la manipulación de los mismos. La mayoría de los sistemas que emplean tarjetas de banda magnética deben de tener conexiones en línea a los servidores del sistema a pesar de que esto genera costos importantes para las transmisiones de los datos requeridos.

Los enormes progresos de la microelectrónica en la década de 1970, hizo posible la integración del almacenamiento de datos y la lógica de procesamiento de los mismos en un chip de material semiconductor de pocos milímetros cuadrados.

El primer progreso real en el desarrollo de las tarjetas inteligentes se produjo cuando Roland Moreno registró sus patentes de tarjetas inteligentes en Francia en 1974. Fue entonces que la industria de los semiconductores fue capaz de suministrar los circuitos integrados necesarios a precios aceptables.

Un proyecto piloto se llevó a cabo en Alemania en 1984-85, el uso de tarjetas de teléfono basado en varias tecnologías. Tarjetas de banda magnética, de almacenamiento óptico (holográfica) y tarjetas inteligentes se utilizaban en las pruebas comparativas. Las tarjetas inteligentes demostraron ser las ganadoras de este proyecto piloto.

La tecnología EPROM (erase programmable read only memory por sus siglas en inglés) represento mayores beneficios y mejor economía, la cual fue utilizada en

los chips de las tarjetas de teléfonos franceses, chips de EEPROM (erase electrical programmable only memory) más recientes se utilizaron desde el principio en las tarjetas telefónicas alemanas.

En 1986, varios millones de tarjetas inteligentes telefónicas estaban en circulación sólo en Francia. El total se elevó a casi 60 millones en 1990, y en varios cientos de millones en todo el mundo en 1997. Alemania experimentó un avance similar, con un tiempo de retraso de unos tres años. Estos sistemas se comercializan en todo el mundo después de la exitosa introducción de la tarjeta inteligente de telefonía pública en Francia y Alemania.

Los circuitos integrados que se utilizan en las tarjetas de teléfonos son relativamente pequeños, sencillos y de bajo costo. Los chips de memoria con una lógica de seguridad específica permiten se realice al mismo tiempo la protección del saldo de la tarjeta y la protección de la operación cotidiana.

Los chips de los microprocesadores, que son significativamente más grandes y de lógica más compleja, se utilizaron por primera vez en un gran número de aplicaciones de telecomunicaciones, en particular para las telecomunicaciones móviles. En 1988, la oficina de correos alemán, actuó como un pionero en esta área al introducir un moderno microprocesador de tecnología PROM (programable read only memory por sus siglas en inglés) como tarjeta de autorización de la red de telefonía móvil analógica.

El progreso es significativamente menor en el ámbito de las tarjetas bancarias, en parte debido a su mayor complejidad operativa y de seguridad, en comparación con las tarjetas telefónicas. Aquí es importante señalar que el desarrollo de la criptografía moderna ha sido crucial para la proliferación de las tarjetas bancarias así como la evolución de la tecnología de los semiconductores.

Con la expansión general del procesamiento electrónico de datos en la década de 1960, la disciplina de la criptografía refleja una especie de salto cuántico. El hardware y el software que se puede instalar en los equipos permiten llevar a cabo complejos y sofisticados algoritmos matemáticos que brindan niveles sin precedentes de seguridad. Por otra parte, esta tecnología está disponible en todo el mundo, en contraste con la situación anterior en la que la criptografía era una ciencia secreta reservada de manera privada de los servicios militares y secretos.

La tarjeta inteligente representa ser un medio ideal con un alto nivel de seguridad (basada en la criptografía) a disposición de todos, ya que puede almacenar de forma segura las claves secretas y ejecutar algoritmos criptográficos. Además, las tarjetas inteligentes son pequeñas y fáciles de manejar que pueden ser transportadas y utilizadas en todas partes por todo el mundo en la vida cotidiana.

Los bancos franceses fueron los primeros en introducir esta tecnología en 1984, tras un ensayo con 60.000 tarjetas durante 1982 y 1983. Tuvieron que pasar otros 10 años antes de que todas las tarjetas de los bancos franceses incorporaran chips.

En Alemania, las primeras pruebas de campo se llevaron a cabo en 1984 y 1985, con una tarjeta de pago multifuncional que incorpora un chip. Sin embargo, la Kreditausschuss Zentrale (ZKA), que es el comité de coordinación de los principales bancos alemanes, Eurocheque no logró emitir una especificación de tarjetas multifuncional que incorporará chips hasta 1996.

En 1997, todas las instituciones de ahorro y los bancos alemanes emitieron las nuevas tarjetas inteligentes. En el año anterior, las tarjetas multifuncionales inteligentes con funciones de punto de venta, monedero electrónico un servicio de valor añadido opcional, se emitió en toda Austria. Esto hizo que Austria fuera el primer país del mundo en implementar un sistema nacional de monedero electrónico.

Un hito importante en todo el mundo para el futuro de las tarjetas inteligentes en el uso de efectuar los pagos con ella fue la conclusión de las especificaciones EMV, que representa el producto de los esfuerzos conjuntos de Europay, Master Card y Visa. La primera versión de esta especificación se publicó en 1994.

Esta especificación contiene descripciones detalladas de las tarjetas de crédito que incorporen chips de microprocesadores, y que garantiza la compatibilidad recíproca de las tarjetas inteligentes del futuro.

Los sistemas de monedero electrónico siguen demostrando ser otro factor importante en la promoción internacional del uso de las tarjetas inteligentes para las transacciones financieras. El primer sistema, llamado Danmønt, fue puesto en funcionamiento en Dinamarca en 1992. El uso de estos sistemas también es cada vez mayor fuera de Europa. En los EE.UU., donde los sistemas de tarjetas inteligentes se tardaron en establecer, Visa experimentó con una tarjeta inteligente durante los Juegos Olímpicos de Verano en Atlanta en 1996.

Varios países europeos ya trabajan con sistemas de firma electrónica, después de haber sido elaborado un fundamento jurídico para el uso de firmas electrónicas, el cual ya está aprobado mediante una directiva europea en materia de firma electrónica en 1999.

Las tarjetas inteligentes también están siendo utilizadas como "boletos electrónicos" para el transporte público local en muchas ciudades de todo el mundo. El sistema de prepago más grande del mundo, Octupus en China, es un ejemplo de éxito de este tipo de aplicación.

Los factores socioeconómicos que impulsan el desarrollo de las tarjetas inteligentes fundamentalmente son los aspectos de la seguridad de la información contenidas en ellas, mientras que los factores tecnológicos que la impulsan son el desarrollo de la microelectrónica, la criptografía y la estandarización de las especificaciones.

Como puede verse en el resumen histórico, las posibles aplicaciones para las tarjetas inteligentes son muy diversas. Con la capacidad de almacenamiento cada vez mayor y la capacidad de tratamiento de los circuitos integrados disponibles, la gama de posibles aplicaciones se está ampliando constantemente. Dado que es imposible describir todas estas aplicaciones en detalle dentro de los límites de este trabajo unos pocos ejemplos típicos sirven para ilustrar las propiedades básicas de las tarjetas inteligentes.

2.2 Tecnología de tarjetas inteligentes

Esta sección describe los conceptos básicos y la definición de términos fundamentales de las tarjetas inteligentes.

2.2.1 Tipos de tarjetas con chip

A menudo, los términos "tarjeta inteligente", "tarjeta de circuito integrado" y "tarjetas con chip" se utilizan indistintamente, pero pueden significar diferentes cosas. Las tarjetas se distinguen tanto por el tipo de chip que contienen como por el tipo de interfaz que usan para comunicarse con el lector.

Existen tres tipos diferentes de chips que pueden estar asociados con estas tarjetas: sólo de memoria, que incluye la memoria protegida, de lógica cableada y de microprocesador

2.2.1.1 Tarjetas de chip de circuito integrado solamente de memoria

Tarjetas únicamente de memoria son de “banda magnética electrónica”, proporcionan más seguridad que las tarjetas de banda magnética. Las dos ventajas que tienen sobre las de banda magnética son:

a) Tienen mayor capacidad de almacenar datos y,
b) Existen más dispositivos de lectura/escritura

Las tarjetas de chip sólo de memoria no contienen lógica ni permiten realizar cálculos. Ellas simplemente almacenan datos.

Esta versión de tarjetas, son únicamente de lectura y de baja capacidad. Nuevas versiones incluyen disponibilidad de prepago que usan memoria de lectura/escritura y esquemas de conteo binario que permiten a las tarjetas ser empleadas en servicios de transporte.

Muchas de estas tarjetas también son desarrolladas para ser protegidas a través del uso del número de identificación personal (Pin), y contadores, con límite del número de veces que el monedero puede ser recargado.

2.2.1.2 Tarjetas con chip de circuitos integrados con lógica cableada

El circuito de la tarjeta contiene un chip basado en la lógica de una máquina de estados, que proporciona el cifrado y autenticación de acceso a la memoria y a su contenido. La lógica de las tarjetas de conexión por cable, ofrecen un sistema de archivos estáticos como apoyo a múltiples aplicaciones, así como cifrado opcional con acceso a los contenidos de la memoria. Sus sistemas de archivo y conjunto de comandos sólo se pueden cambiar mediante el rediseño de la lógica del CI.

2.2.2 El chip con microprocesador seguro

Un chip con microprocesador seguro tiene: una unidad de procesamiento central (CPU) de 8 a 32 bits, una memoria de sólo lectura (ROM) o memoria flash que contiene el sistema operativo del chip y, opcionalmente, software de aplicación; memoria de acceso aleatorio (RAM) que sirve como un registro temporal de datos; memoria no volátil que se utiliza para el almacenamiento de datos de usuario (por ejemplo, programas y memoria de sólo lectura (EEPROM), ferro eléctricos RAM, memoria flash; donde se integran las medidas de seguridad contra las amenazas conocidas y previstas para alcanzar los niveles de seguridad de Common Criteria o el estándar de certificación FIPS 120, sensores de ambiente (por ejemplo, voltaje, frecuencia, temperatura); al menos un puerto de comunicaciones serie; un generador de números aleatorios; temporizadores; motor de cifrado opcional (por ejemplo, DES, 3DES, RSA); otros periféricos opcionales dedicados (por ejemplo, control del acelerador criptográfico, interfaz serial periférica, puerto de comunicación).

De manera resumida los tipos de memoria son:

ROM (Read Only Memory). Memoria de sólo lectura contiene el sistema operativo del chip. El sistema operativo o conjunto de comandos de los controles de todas las comunicaciones entre el chip y el mundo exterior. El sistema operativo controla el acceso al sistema de archivos o applets. La ROM está enmascarada o escrita durante la producción por el fabricante de semiconductores y, una vez escrito, no puede ser alterado.
EEPROM (Erase Electrical Programmable Read Only Memory). Memoria eléctricamente borrable programable sólo de lectura; es la memoria no volátil (es decir, que no pierde sus datos si la energía está apagada) y es memoria de lectura/escritura para el almacenamiento de datos. El acceso a la memoria EEPROM es controlado por el sistema operativo del chip.

La EEPROM puede contener datos tales como un Pin que sólo se puede acceder por el sistema operativo y el número de serie de una tarjeta.

La EEPROM se utiliza normalmente para aplicaciones de datos y para ciertas funciones de filtrado. La mayor parte de la memoria EEPROM se utiliza para almacenar datos del usuario, como las características biométricas, número de cuenta bancaria, autorización de uso especial, registros de lealtad, la información demográfica, y registros de transacciones. La EEPROM se puede escribir decenas a cientos de miles de veces y se puede programar o borrar en cualquiera de los bloques o bytes.
FRAM (RAM ferro eléctrica) es otra tecnología de memoria no volátil. Las memorias FRAM pueden leer datos miles de veces más rápido a un voltaje de alimentación muy inferior a otros dispositivos de memoria no volátil. FRAM es la memoria de acceso aleatorio que combina la rapidez de lectura y escritura de memoria RAM dinámicas (DRAM), la memoria más usada en computadoras personales, con la capacidad de retener datos cuando se apaga (como lo hacen otros dispositivos de memoria no volátil tales como ROM y de memoria flash). Porque FRAM no es tan denso como DRAM y la RAM estática (SRAM) (es decir, no puede almacenar tantos datos en el mismo espacio). Sin embargo, debido a que la memoria es más rápida con un requisito de energía muy bajo, se espera tener muchas aplicaciones en dispositivos pequeños. FRAM es más rápida que la memoria flash.

Memoria Flash (a veces llamado "flash RAM") es un tipo de memoria no volátil a potencia constante, que puede ser borrada y reprogramada en unidades de memoria llamadas bloques. La memoria Flash se utiliza a menudo para mantener el código de control, como el sistema básico de entrada y salida (BIOS) en un ordenador personal.

Algunos fabricantes de chips proporcionan componentes con una combinación de ROM, memoria flash y EEPROM.

RAM (Random Access Memory), memoria volátil, que se utiliza como un registro de almacenamiento temporal por el microprocesador del chip. Por ejemplo, cuando un Pin está siendo verificado, el Pin terminal o el Pin pad se almacena temporalmente en la memoria RAM.

Al evaluar los tipos de tarjeta para una aplicación particular, la cantidad de memoria en diversos componentes es importante. La capacidad de una tarjeta de EEPROM es crítica porque una EEPROM de mayor capacidad puede almacenar un mayor número de registros de aplicaciones y archivos de transacciones. La capacidad de la ROM también es importante porque una ROM de mayor capacidad puede contener un sistema operativo más sofisticado, lo que facilita a la tarjeta operaciones complejas del sistema.

También hay una relación entre la ROM y EEPROM en algunas tarjetas, porque algunos fabricantes permiten que el código personalizado extienda el sistema

operativo de la ROM a la EEPROM. Esta técnica aumenta la funcionalidad de la tarjeta, aunque disminuye la cantidad de EEPROM disponible para la aplicación y almacenaje de la transacción. Por el contrario, solicitudes establecidas y aceptadas se pueden incluir en la memoria ROM de las versiones futuras de chips, liberando espacio de memoria EEPROM para aplicaciones adicionales y de expansión.

2.2.2.1 Tarjetas de chip con microprocesador de seguridad integrado

Las tarjetas con microprocesador contienen un microprocesador, un sistema operativo y memoria de lectura/escritura que puede ser actualizada varias veces.

La tarjeta de chip con microprocesador con seguridad, contiene los medios de almacenamiento de datos y ejecuta la lógica y los cálculos de conformidad con su sistema operativo. Todo lo que necesita para operar es el suministro de energía y una terminal de comunicación. Las tarjetas de chip con microprocesadores pueden ser de contacto, sin contacto y de microprocesadores de ambos circuitos integrados de interface. A diferencia de la tarjeta sólo de memoria, los productos del microprocesador están diseñados y pueden ser verificados para cumplir los objetivos de seguridad, como los que establece ISO/IEC 15408 [W15] Common Criteria. La tarjeta de chip con microprocesador con seguridad es normalmente la versión conocida como la "tarjeta inteligente".

2.2.2.2 Interfaces de tarjetas inteligentes con contacto y sin contacto

Siguiendo con el Government Smart Card Handbook [R2] y [R20], las tarjetas inteligentes pueden interactuar con dispositivos de lectura/escritura ya sea por contacto eléctrico directo con la tarjeta o mediante transferencia inalámbrica de datos (es decir, sin contacto de interacción) por radiofrecuencia o técnicas de acoplamiento de inducción. La interfaz de contacto requiere que la tarjeta se inserte en un lector de tarjetas para que el lector pueda establecer un contacto eléctrico directo con el chip.

Una tarjeta inteligente sin contacto contiene un chip y una antena colocada entre dos capas de plástico. La comunicación se realiza mediante la tecnología de radiofrecuencia. El chip se alimenta a través de la antena de la tarjeta cuando la tarjeta se coloca dentro de los 10 centímetros desde el lector de tarjetas inteligentes. Las tarjetas de contacto se utilizan generalmente para una amplia variedad de aplicaciones, incluidas las transacciones financieras y de control de acceso lógico. Las tarjetas sin contacto se utilizan normalmente para funciones que requieren una mayor velocidad y facilidad de operación (por ejemplo, alto volumen de tránsito de los sistemas automatizados de tarifa de cobro o de acceso a los edificios).

Tarjetas con interfaces de contacto y sin contacto pueden soportar múltiples aplicaciones, que ofrecen ventajas tanto a la organización que expide la tarjeta

como al titular de la tarjeta. La organización que las expide puede consolidar una combinación adecuada de tecnologías y el apoyo a una variedad de políticas de seguridad para diferentes situaciones. Aplicaciones tales como el acceso lógico a las redes informáticas, pago electrónico, boletaje electrónico, y el tránsito puede ser combinado con el acceso físico en una multiaplicación y multitecnología de identificación de credenciales.

Con tarjetas híbridas y de doble interface, los emisores también pueden implementar sistemas que se benefician de las interfaces de tarjetas múltiples.

Hay tres principales tecnologías sin contacto para el control de acceso: ISO/IEC 14443, ISO/IEC 15693 y tecnologías 125 kHz.

Las tarjetas sin contacto que se ciñen al estándar ISO/IEC 14443 e ISO/IEC 15693 trabajan en el rango de 13.56 mHz.

Las tarjetas sin contacto que se ciñen al estándar ISO/IEC 14443 son compatibles con el estándar ISO/IEC 7816.

Las tarjetas sin contacto que se ciñen al estándar ISO/IEC 15693, no son compatibles con ISO/IEC 7816, fueron desarrolladas para aplicaciones de logística (inventarios), etiquetado y aplicaciones de agricultura donde pequeñas cantidades de datos necesitan transferirse grandes distancias.

Las tecnologías 125 kHz de sólo lectura, son usadas principalmente por los sistemas de control de acceso vía RFID. Las tecnologías 125kHz permiten que un número de código sea transmitido y procesado por un sistema de soporte. Este sistema determina los derechos y privilegios asociados con la tarjeta.

2.2.2.3 Tarjetas inteligentes híbridas

Una tarjeta híbrida contiene dos chips, uno para la interfaz de contacto y otro para la interfaz sin contacto. Las placas que soportan los chips en la tarjeta suelen no estar conectadas entre sí.

2.2.2.4 Tarjetas inteligentes con interfaz dual

Una tarjeta con chip de interfaz dual contiene un chip que soporta las interfaces de contacto y sin contacto.

Estas dos interfaces en la tarjeta proporcionan la funcionalidad de contacto y sin contacto de forma única, con diseños capaces de permitir que la misma información se accese a través de lectores con contacto o sin contacto.
De acuerdo a este apartado, podemos decir, que con base a los requerimientos y especificaciones de las aplicaciones a instalar en las tarjetas inteligentes, será la selección del tipo de chip e interfaces que deba de contener. Esta información

estará contenida en los diccionarios de los perfiles de las tarjetas y aplicaciones, los cuales serán administrados por el sistema de gestión de tarjetas inteligentes.

2.3 Características físicas y eléctricas de los microprocesadores

2.3.1 Propiedades eléctricas de las tarjetas

Las propiedades eléctricas de las tarjetas inteligentes están establecidas en el estándar ISO/IEC 7816, el cual precisa el tamaño y posición de los contactos, los voltajes de alimentación, el consumo de corriente máxima y las señales de las secuencias de activación y desactivación.

Debido a la gran cantidad de tarjetas inteligentes utilizadas en el sistema GSM (por sus siglas en inglés global system for mobile communications), las especificaciones de las características eléctricas para las tarjetas GSM son las directrices generales para todos los fabricantes de microprocesadores de tarjetas inteligentes

Se puede suponer que casi todos los nuevos microprocesadores para tarjetas inteligentes cumplen con los parámetros generales eléctricos de las especificaciones GSM, ya que de lo contrario serían prácticamente invendibles en el mercado de las telecomunicaciones.

Con un gran número de aplicaciones, donde varios tipos de tarjetas inteligentes deben trabajar en conjunto con diferentes tipos de terminales, es un requisito ineludible que todas las tarjetas que se utilizan sean eléctricamente idénticas o al menos, se comporten de manera uniforme dentro de los rangos eléctricos claramente definidos. La base general internacional de las propiedades eléctricas de las tarjetas inteligentes es el estándar ISO/IEC 7816-3.

El estándar 7816-1 proporciona una gama de opciones que, en muchos casos es demasiado extensa para uso práctico. Esto permitió que normas de la industria las complementaran, como es el caso de la norma EMV 2000 para las transacciones financieras y para algunas de la familia de la norma GSM 11.X empleada para aplicaciones de telecomunicaciones. Estas normas de la industria de ninguna manera compiten con la norma ISO/IEC 7816-1 sino que se complementan con restricciones significativas derivadas de las aplicaciones prácticas de las tarjetas inteligentes utilizadas en millones de las tarjetas emitidas.

Como lo describe Wolfgang Ranki [17], la tabla 1 presenta un resumen de las necesidades eléctricas más importantes de las normas internacionales y de la industria.

2.3.2 Conexiones eléctricas

El estándar 7816-2 señala que las tarjetas inteligentes pueden tener 6 u 8 contactos, los cuales constituyen la interfaz eléctrica entre la terminal y el microprocesador en la tarjeta. Sin embargo, este estándar establece que dos de los ocho contactos (C4 y C8) están reservados para contactos auxiliares AUX1 y AUX2, que pueden ser utilizados en el futuro para interfaces.

En la actualidad, algunos módulos de tarjeta inteligente sólo tienen seis contactos,

Tabla 1. Parámetros de variables eléctricas de microprocesadores

Estándar y clase	**Voltaje**	**Rango de reloj**	**Corriente máxima**
ISO/IEC 7816-3 Clase A Clase B Clase C Clase A,B y C con reloj detenido	 5V +-10% 4.5-5.5V 3v+-10% 2.7-3.3V 1.8V+-10%1.62-1.98 V	 1-5 MHz 1-5Mhz 1-5 MHz	 60mA a 5 MHz 50mA a 4 MHz 30mA a 4Mhz .5 mA (reloj detenido)
EMV 2000	5v+-10%4.5-5.5v	1-5Mhz	50mA para todos los rangos de reloj

ya que en estos contactos, hasta finales de 1980, era necesario aplicar una tensión externa para programar y borrar la EEPROM, puesto que los microprocesadores de entonces no tenían área de carga. El contacto C6 estaba reservado para este propósito. Sin embargo, desde de la década de 1990 es práctica normal generar este voltaje directamente en el chip usando un contacto de carga, por lo que este contacto ya no es utilizado. Sin embargo, no puede ser empleado para alguna otra función puesto que entraría en conflicto con lo dispuesto en esta norma ISO 7816. La tabla 2 muestra la designación de los contactos y sus funciones

Tabla 2. Designación de los contactos y funciones de acuerdo a la norma ISO 7816-2

Contacto	**Designación**	**Función**
C1	Vcc	Voltaje de alimentación
C2	RST	Reinicio de entrada
C3	CLK	Reloj de entrada
C4	AUX1	Contacto complementario auxiliar 1
C5	GND	Tierra
C6	Vpp	Voltaje de programación

Contacto	Designación	Función
C7	I/O	Entrada/Salida para comunicaciones seriales
C8	AUX2	Contacto suplementario auxiliar 2

2.3.3 Voltaje de alimentación

El voltaje de alimentación para las tarjetas inteligentes originalmente fue de 5 volts, con una tolerancia máxima de ± 10%.

En las normas internacionales la gama de voltaje de las tarjetas inteligentes está considerado el rango de 3 a 5 volts, con una tolerancia de ± 10%. Esto da un alcance efectivo de 2,7 a 5,5 volts.

La norma ISO/IEC 7816-3 y su modificación definen tres clases para los rangos de voltaje de las tarjetas inteligentes. La Clase A abarca el rango de voltaje de 5 volts ± 10%, la Clase B cubre el rango de 3 volts ± 10% y la Clase C cubre el rango de 1.8 volts ± 10%. Las tres clases pueden ser utilizadas individualmente o en cualquier combinación deseada. Por ejemplo, si una tarjeta inteligente que cumple con los requisitos para la clase A y la B, puede ser utilizada con 5 y 3 volts de alimentación. Sin embargo, debe tenerse en cuenta que el rango entre 3,3 volts y 4,5 volts se encuentra fuera de los intervalos especificados, por lo que la tarjeta inteligente no tiene necesariamente que ser capaz de operar en este rango.

Sin embargo, las tarjetas inteligentes por lo general se pueden utilizar sin problemas entre los límites superior e inferior de los rangos de voltaje especificado.

La norma ISO/IEC 7816-3 impone otro requisito igualmente importante, el cual señala que bajo ninguna circunstancia se puede dañar el microprocesador de una tarjeta inteligente, si la tarjeta se alimenta de voltaje que no es compatible con el microprocesador. Éste es un requisito esencial para garantizar la compatibilidad ascendente de nuevos tipos de tarjetas inteligentes con los principales tipos de terminales.

El objetivo es eliminar la posibilidad de que el uso de un contacto de 3 volts en una terminal de 5 volts, por ejemplo, podría destruir el CI de la tarjeta.

La situación de las tarjetas inteligentes utilizadas en el ámbito de las telecomunicaciones es completamente diferente. Desde finales de la década de 1990, 3 volts se ha convertido en el voltaje de funcionamiento estándar para los dispositivos GSM.

2.3.4 Corriente de alimentación

La primera versión de la norma ISO/IEC 7816-3 de 1989, establecía una corriente máxima de 200 mA con un voltaje de alimentación de 5 volts y 5-MHz, pero incluso entonces era demasiado. Desde entonces, los valores han sido reducidos significativamente y ahora depende de las distintas clases de voltaje de suministro. El factor más importante es el consumo real de un microprocesador, el cual es directamente proporcional a la frecuencia. También depende de la temperatura del microprocesador. La versión actual de ISO/IEC 7816-3 especifica una corriente máxima de tensión de 60mA para la clase A (5 V) a una frecuencia de reloj máxima de 5 MHz y una temperatura ambiente máxima de 50 ◦ C.

Con respecto a las tarjetas inteligentes para las transacciones financieras, en la especificación 2000 de EMV e ISO/IEC 7816-3, el valor de la corriente máxima se reduce de 60 mA a 50 mA, no hay otras importantes restricciones adicionales.

Los microprocesadores modernos para tarjetas inteligentes tienen consumos en el orden de 350 μA por MHz de frecuencia de reloj. Utilizando este valor, podemos escribir la siguiente fórmula para el consumo actual de un microprocesador en función de la frecuencia de reloj o la frecuencia de reloj generada dentro del chip:

$$I = f / 2.87514 \ [ma/MHZ]$$

Esta fórmula es útil para hacer las estimaciones iníciales, pero hay que recordar que el valor nominal del consumo no sólo depende de la frecuencia de reloj, sino también del voltaje de alimentación, la temperatura y por supuesto el tipo de chip.

Todos los microprocesadores de las tarjetas inteligentes tienen varias formas de ahorro. El principio operativo de estas formas se basa en la desactivación de todos los componentes funcionales del chip que no están siendo utilizados. En principio, solamente la interrupción de la lógica de la interfaz E/S, el procesador de los registros y la memoria RAM tienen la necesidad de disponer de voltaje de alimentación con el fin de guardar el estado operativo.

En la práctica, el procesador debe de tener energía también, pero la ROM y la EEPROM están apagados. Cuando el microprocesador está en este modo de sueño o estado de inactividad, su consumo nominal operativo se cae dramáticamente, ya que la mayor parte de los chips están aislados del voltaje de alimentación. Además en este modo de espera, muchos microprocesadores de tarjeta inteligente soportan que el reloj pueda estar apagado, esto es llamado el 'modo de parada de reloj ". El objetivo principal de este modo es permitir que los componentes de hardware de la terminal que generan el reloj se apagué, por lo que este modo hace particularmente atractivo el empleo de pilas para dispositivos terminales. De acuerdo con la norma ISO/IEC 7816-3, el máximo valor real

permitido en el modo de espera con el reloj parado es de 500 µA para las tres clases. Incluso este valor es demasiado alto para el área de las telecomunicaciones móviles. Por ejemplo, GSM 11.11 especifica un límite máximo de 200 µA de 5 volts para las tarjetas inteligentes en una frecuencia de reloj de 1 MHz

Los microprocesadores actuales emplean tecnología CMOS (complementary metal oxide semiconductor por sus siglas en inglés). Bajo ciertas condiciones, grandes corrientes de cortocircuito pueden ocurrir brevemente durante los procesos de conmutación de los transistores. Estos producen picos de corriente que son muchas veces mayores que los valores nominales de funcionamiento, con una duración en el rango de nano segundos. Estos picos pueden también producirse cuando el contacto de carga del EEPROM se enciende. Si la terminal no puede proporcionar estas grandes corrientes durante estos intervalos cortos, el voltaje de alimentación caerá por debajo del valor permitido. Esto puede producir un error de escritura en la EEPROM o activar el detector de reducción de voltaje en el chip. Por esta razón, las referencias a los picos se pueden encontrar en prácticamente todos los estándares y especificaciones pertinentes. Por ejemplo, la ISO/IEC 7816-3 requiere de fuentes de energía para la clase-A (5-V) que sean capaces de manejar los picos con una duración máxima de 400 ns y un máximo de amplitud de 100 mA. Suponiendo un pico triangular, esto equivale a una carga de 20 nano segundos que debe ser suministrado.

Por estas consideraciones, en el diseño de un programa de tarjetas inteligentes es muy importante tomar en cuenta el ambiente de operación de la terminal que estará en contacto con la tarjeta.

2.3.5 Transmisión de datos

Si ocurre un error durante la transmisión de datos, puede suceder que la terminal y la tarjeta intenten enviar datos al mismo tiempo. Esto resulta en una colisión de datos sobre la línea de conexión de E/S. Aparte de los problemas que esto provoca en el nivel de la aplicación, en el nivel físico podría producir corrientes en la línea E/S que podrían ser lo suficientemente grandes como para destruir la interfaz de los componentes.

En combinación con las especificaciones convenidas de no enviar una señal activa de 5 volts, esto evita cualquier problema que podría ocurrir si las dos partes trataran de enviar a la línea de datos dos diferentes niveles de voltaje, como resultado de un error de comunicación.

2.3.6 Secuencias de los microprocesadores

Como lo refiere el estándar 7816 parte 3, todos los microprocesadores de tarjetas inteligentes están protegidos contra cargas electrostáticas y potenciales en los

contactos. Con el fin de evitar estados indefinidos, se deben precisar las especificaciones de las secuencias de activación y desactivación, las cuales se deben cumplir estrictamente. Esto también se refleja en la parte pertinente del estándar ISO/IEC 7816-3. Estas secuencias definen los aspectos eléctricos de la activación y la desactivación de la tarjeta y no tienen nada que ver con la secuencia de establecer contacto mecánico con la tarjeta. Sin embargo, es recomendable poner en contacto mecánico por primera vez el contacto con la tierra de la tarjeta inteligente, como una medida de precaución a fin de garantizar que se encuentre bien definida la conexión eléctrica de desconexión.

El componente central de una tarjeta inteligente es el microprocesador. Controla, inicia y supervisa todas las actividades de la tarjeta. Los microprocesadores que son especialmente diseñados y desarrollados para este propósito son equipos completos en su propio contexto. Esto significa que contienen procesadores, memoria e interfaces con el mundo exterior.

Los componentes funcionales más importantes del microprocesador típico de tarjetas inteligentes son el procesador, los buses de dirección y de datos, y los tres tipos de memoria (RAM, ROM y EEPROM). El chip tiene también una unidad de interfaz que permite la comunicación en serie con el mundo exterior. En el caso más simple, la interfaz en serie es una dirección que puede ser dirigida por la CPU y se conecta al contacto de E/S.

Además, algunos fabricantes proporcionan procesadores especiales en el chip que actúan como coprocesador matemático, si bien se limitan las funciones proporcionadas por estos componentes a las operaciones exponenciales y de módulo de enteros. Ambas de estas operaciones son fundamentales y son elementos necesarios para los procedimientos de cifrado de clave pública, tales como el algoritmo RSA.

Los microprocesadores utilizados en las tarjetas inteligentes no son estándar, existen con una amplia variedad de componentes.

La superficie de la oblea de silicio del microprocesador es uno de los factores decisivos con lo que respecta a los costos de fabricación. El área del chip debe ser lo más pequeña posible. Además, muchos dispositivos estándar comercialmente disponibles, incluyen funciones que no son necesarias en las tarjetas inteligentes. Dado que estas funciones ocupan espacio extra en la oblea se pueden eliminar a partir de chips diseñados para tarjetas inteligentes.
Debido a la necesidad de integrar todos los componentes funcionales de un ordenador en un chip de silicio el número disponible de los dispositivos semiconductores adecuados es limitado. Además, el chip debe contener una memoria que puede ser escrita y borrada, pero que no requiere una fuente de alimentación permanente de los datos (retención de EEPROM o Flash EEPROM).

Para la seguridad de las tarjetas inteligentes, se utilizan principalmente las áreas relacionadas con la seguridad que requieren tanto características pasivas como activas en el chip.

2.3.7 Área de chip

El tamaño del microprocesador afecta fuertemente la fragilidad de los chips. Una mayor zona muerta es más propensa a quebrarse cuando la tarjeta está doblada o retorcida. Por la política de seguridad de los fabricantes de tarjetas, es que los microprocesadores que se utilizan no están disponibles en el mercado abierto. Esto hace que sea mucho más difícil analizar el hardware del chip, ya que un ataque potencial normalmente no tiene acceso a él. Sin embargo, esta posición se ve seriamente debilitada por la disponibilidad general de tarjetas inteligentes programables, como los tipos de Java Card, que por lo general son defendibles para aplicaciones estándar.

2.3.8 Tipos de procesadores

Los procesadores utilizados en las tarjetas inteligentes no son diseños especiales, son empleados una vez comprobado que los dispositivos funcionan en otras áreas por un largo tiempo. En esta industria, no es habitual desarrollar nuevos procesadores para áreas de aplicación especial, ya que esto es generalmente demasiado caro. Además, daría un procesador completamente desconocido, para los que las librerías de funciones y herramientas de desarrollo no estarían a disposición de los desarrolladores de sistemas operativos. Además, los procesadores de la tarjeta inteligente deben ser extremadamente fiables. Por tanto, es mejor confiar en procesadores de tipo más antiguo que demuestran cotidianamente su eficacia en la práctica, en lugar de experimentar con los últimos desarrollos de fabricantes de semiconductores. La industria aeroespacial, que está muy interesada en la seguridad, utiliza componentes que son de una o dos generaciones atrás del estado actual de la tecnología, por las mismas razones.

Microprocesadores de tarjetas inteligentes en el extremo inferior de la escala de rendimiento suelen tener una memoria direccionable en el rango de 6 KB a 30 KB. En estas condiciones, utilizando un bus de memoria de 8-bit no impone ninguna restricción significativa. Los procesadores utilizados generalmente tienen una arquitectura de conjunto complejo de instrucciones de computadora (CISC por sus siglas en inglés), lo que significa que se requieren de varios ciclos de reloj para ejecutar instrucciones de la máquina y suelen tener conjuntos de instrucciones muy grandes. El rango de direcciones más frecuente es de 8 a los 16 bits, que permite hasta 65.536 bytes que pueden direccionarse.

Los procesadores de la familia de 8 bits también están disponibles con ampliaciones que les permiten hacer frente a los bancos de memoria adicional, a fin de superar el límite de 64 Kb. El acceso a la memoria de estos bancos es controlado a través de registros especiales de los mapas de memoria en una

región de memoria específica, donde se puede acceder por el procesador. Sin embargo, este tipo de memoria no-lineal tiene desventajas significativas. Por ejemplo, la distribución relativamente compleja de código de programa en varios bancos de memoria complica considerablemente el software, aumentando así la probabilidad de los errores. La memoria adicional es también necesaria para la funcionalidad de interrupción de banco. En consecuencia, la expansión del espacio de memoria mediante bancos de memoria es ante todo un recurso provisional que se utiliza a la espera de la transición a los procesadores con un ancho mayor de bits.

En el extremo superior de la escala de desempeño para los microprocesadores de tarjetas inteligentes están ya disponibles los de 16 y 32 bits. La tendencia de desarrollo es bastante clara en la dirección de procesadores de 32 bits. Estos procesadores se necesitan a fin de manejar los registros de gran tamaño (superior a los límites de 64 Kb), sobre todo para satisfacer la enorme necesidad de procesamiento de modernos sistemas operativos basados en tarjetas inteligentes, tales como Java Card.

Los criterios clave para la selección de los procesadores incluyen la densidad de código, la disipación de potencia y la resistencia a los ataques.

A pesar de que los procesadores de 32 bits ocupan mucho más espacio que los procesadores de 8 bits que están desapareciendo, usan la misma tecnología con buses más amplios y con estructuras internas más complejas, son utilizados cada vez más en un número mayor de aplicaciones de tarjetas inteligentes. El poder de procesamiento que ofrecen es indispensable para estas aplicaciones, de modo que los inconvenientes de mayor poder de consumo y el aumento del área del chip pueden ser aceptados como el precio del progreso.

2.3.9 Hardware complementario

Hay algunos requisitos específicos de las tarjetas inteligentes que no pueden atenderse plenamente con el uso del software y por lo tanto deben ser satisfechos por el hardware adicional, ya que no pueden ser satisfechos mediante el hardware de los microprocesadores convencionales.

En consecuencia, los distintos fabricantes de microprocesadores de tarjetas inteligentes ofrecen una amplia gama de funciones complementarias del chip del hardware. Los componentes más utilizados para las funciones complementarias son los que se describen a continuación.

Es económicamente razonable integrar un coprocesador RSA en un microprocesador cuyo objetivo de la aplicación utiliza algoritmos criptográficos asimétricos.

Otro aspecto de la funcionalidad complementaria con respecto a microprocesadores

de tarjetas inteligentes se relaciona con el tema de la seguridad, en las descripciones de funciones adicionales implementadas en el hardware que tienen como principal objetivo contrarrestar posibles ataques.

Basada en hardware de transmisión de datos, las comunicaciones entre una tarjeta inteligente y el mundo exterior se lleva a cabo a través de una interfaz serie bidireccional. Originalmente, la transmisión y recepción de datos a través de esta, es controlada exclusivamente por el software del sistema operativo, sin ningún tipo de soporte de hardware. Esto requiere de software muy complejo, y crea nuevas fuentes de errores potenciales de software. Sin embargo, el problema principal es que limita la velocidad de la transmisión de datos basado en software, ya que la velocidad del procesador es limitada.

Si una mayor velocidad de comunicación es necesaria, se requiere utilizar la multiplicación de reloj interna o un componente receptor/transmisor asíncrono universal (UART por sus siglas en inglés). Este elemento es un componente de propósito general para la transmisión y recepción de datos independiente del procesador. No está limitado por la velocidad del procesador, no necesita software para la comunicación a nivel de byte.

Muchos de los nuevos tipos de microprocesadores también permiten una interfaz USB para ser colocados en el chip como un componente opcional, además de una interfaz UART. Con una sería posible el intercambio de datos con una terminal usando el protocolo USB con soporte de hardware.

La parte 12 de la norma ISO/IEC 7816 establece los requisitos de conformidad y lineamientos para interfaces USB.

Fichas técnicas de los microprocesadores para tarjetas inteligentes se encuentran en los sitios [W24], [W25], [W26], [W27] y [W28].

2.4 Sistemas operativos de tarjetas inteligentes

De acuerdo con Tapiador [2], el sistema operativo de las tarjetas inteligentes, proporciona una interfaz de comandos de alto nivel que facilitan su uso. De manera genérica realizan las siguientes funciones:

- Impiden la ejecución de instrucciones hasta que no se haya ejecutado una instrucción especifica
- Al recibir un “reset”, inicializa los parámetros de la tarjeta, da una respuesta y espera la recepción de una instrucción por parte del mundo exterior
- Al recibir una instrucción:
    - Comprueba que es una instrucción válida
    - Comprueba que sus parámetros están bien definidos
    - Verifica las condiciones de seguridad
    - Verifica el estado de los datos referidos dentro de la tarjeta

- Si todas las verificaciones son positivas, ejecuta la instrucción y devuelve una respuesta
- Si alguna verificación es negativa, declara un error al exterior

Los servicios prestados por un sistema operativo de tarjeta inteligente se pueden resumir en:

- Controla el intercambio con el mundo exterior
- Gestiona el manejo de la memoria y de los datos
- Gestiona los mecanismos y servicios de seguridad
- Controla las fases del ciclo de vida de la tarjeta

El sistema operativo es lo que transforma a una placa de plástico con un procesador integrado, su memoria y algunas funciones periféricas en una tarjeta inteligente.

Abundando y de acuerdo a Wolfgang [18], los actuales sistemas operativos de tarjetas inteligentes se almacenan en la memoria ROM del microprocesador de forma inalterable. Utilizan una gran parte de la memoria RAM disponible y una pequeña parte de la EEPROM. Casi todos los sistemas comunes que funcionan en las tarjetas inteligentes se basan en las disposiciones establecidas en la familia del estándar ISO/IEC 7816.

Los sistemas operativos de tarjetas inteligentes se pueden clasificar en los sistemas operativos nativos y sistemas operativos basados en intérpretes.
Sistemas operativos nativos y las aplicaciones que se ejecutan a partir de ellos, se ejecutan en el lenguaje de máquina del procesador asociado. Por lo general son generados en el lenguaje de programación C, y no tienen un intérprete o compilador para traducir los programas en el lenguaje de máquina del procesador destino.

La mayoría de los sistemas operativos basados en intérprete están escritos en lenguaje C, pero los programas de aplicación que se ejecutan en ellos no tienen que ser generados en el lenguaje de máquina del procesador destino. En cambio, pueden ser escritos en un lenguaje de programación interpretado como Java. En consecuencia, estos sistemas operativos incorporan un intérprete para traducir programas en el lenguaje de máquina del procesador de destino. Algunos ejemplos conocidos de sistemas operativos basados en intérprete son Java Card [W8] y MULTOS [W29].

2.4.1 Administración de archivos

La administración de archivos en tarjetas inteligentes está completamente basada en las disposiciones de la norma ISO/IEC 7816-4.

La gestión de archivos es la tarea principal de un sistema operativo de tarjetas inteligentes. La administración de archivos es el suministro del medio para que a través de su acceso se lean, escriban, creen y se borren archivos.
También otorgan la concesión de privilegios de acceso y vigilancia del cumplimiento de los privilegios de acceso. La gestión de archivos es especialmente importante porque la mayoría de aplicaciones de tarjetas inteligentes están basadas en archivos.

2.4.2 Tipos de archivo

Redundando, como lo establece el estándar ISO/IEC 7816 parte 4 y como lo apunta Tapiador [2] los diferentes tipos de archivos que pueden existir son:

- Archivo maestro (MF): Es el directorio raíz de la tarjeta y su identificador es 3F00

- Archivo dedicado (DF): Es la nomenclatura utilizada para referirse a los directorios, es decir, son archivos que en lugar de contener datos, contienen archivos, que a su vez pueden ser del tipo DF. El nivel de profundidad que puede alcanzarse en el árbol de archivos de una tarjeta, depende exclusivamente de su sistema operativo

- Archivo elemental (EF): Es un archivo propiamente dicho, es decir aquel que contiene datos. Dependiendo de su utilización dentro de la tarjeta se puede clasificar en:

    - Internos: Son aquellos archivos tipo EF que son interpretados por la tarjeta para operaciones internas
    - De trabajo: Son el resto de los archivos tipo EF, es decir, los que utiliza el usuario libremente según las condiciones de acceso de diseño de la aplicación

Por otro lado, dependiendo de la estructura que tengan los datos dentro del propio archivo, independientemente de ser interno o de trabajo, los archivos tipo EF pueden ser:

- Transparentes: Son aquellos archivos que no tienen estructura, es decir, todo el tamaño del archivo es un único bloque, donde se puede almacenar datos. Para acceder a un dato hay que indicar en qué posición dentro del archivo se encuentra

- De registros de longitud fija: Son archivos que están estructurados en registros y todos estos tienen una longitud determinada. La referencia a los datos se hace mediante el número de registro en el que se encuentra y el lugar dentro del registro donde se encuentra.

- De registros de longitud variable: Es el mismo caso anterior, pero aquí no se tiene la restricción de la longitud fija para todos los registros. La forma de referenciar es idéntica al caso anterior.

- Cíclicos: Son archivos de registros de longitud fija en los que no existe una referencia absoluta de los registros, es decir, no tiene ni principio ni final, sino que se tiene un apuntador al último registro al que se ha accedido. Para referirse a los datos, hay que hacer movimientos relativos a él, es decir incrementar o decrementar el apuntador. Su uso es fundamental cuando se definen históricos, hasta un máximo, sobre escribiendo la información más antigua cuando se alcanza el tope del archivo. Por lo tanto se mantienen en memoria siempre los últimos movimientos.

- Estructura TLV: En esta estructura, cada objeto de datos es identificado por la etiqueta (T) y longitud (L), elementos, que son seguidos por los datos reales o el valor (V). Esta estructura de archivos también se puede utilizar para almacenar objetos de datos anidados.

De conformidad con ISO/IEC 7816-4 y siguiendo a Wolfgang [18], las estructuras de archivos de las tarjetas inteligentes siempre se basan en una estructura de árbol con un directorio raíz, como se ilustra en la figura 1. El directorio raíz de una tarjeta inteligente, es análoga a la raíz en el volumen de una computadora personal, se llama MF (archivo maestro) y está presente sólo una vez en el árbol de archivos de la tarjeta inteligente. Tiene las propiedades de un directorio, lo que significa que únicamente puede contener otros directorios, y no puede almacenar los datos directamente.

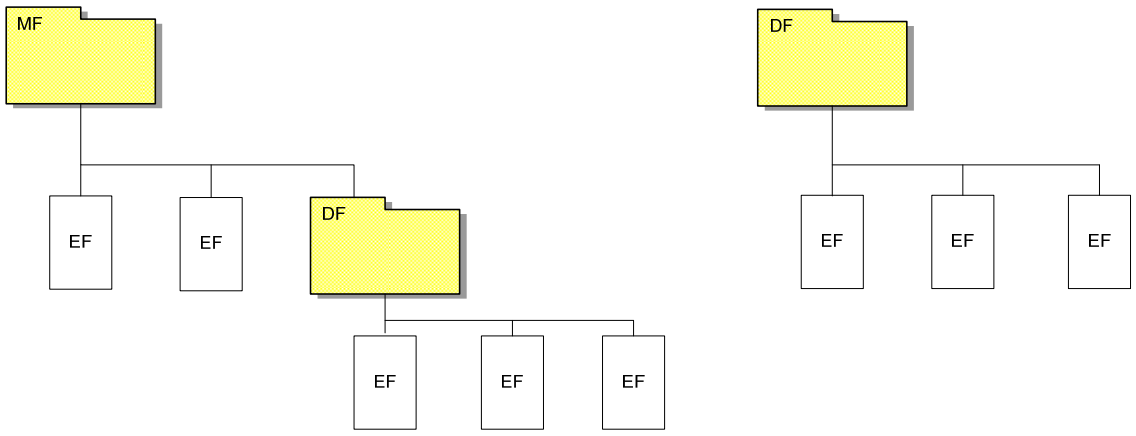


Figura 1. Alternativas para almacenar archivos en tarjetas inteligentes

Los directorios de una tarjeta inteligente se llaman DF (archivos dedicados), y, en teoría, pueden ser anidados indefinidamente. Tres o cuatro niveles se utilizan

comúnmente en aplicaciones reales, los sistemas operativos de tarjetas inteligentes rara vez soportan más de ocho niveles. Los datos de la aplicación del sistema operativo y los datos se almacenan en la EF. La EF siempre se encuentra en los directorios, y hay dos tipos posibles: EF de trabajo y EF interno. El EF de trabajo se utiliza para almacenar los datos de la aplicación que es accesible para el mundo exterior a través de comandos de la tarjeta inteligente. Por el contrario, los EF internos son utilizados por la operación de tarjetas inteligentes para almacenar los datos de fines internos. Por ejemplo, se pueden utilizar para almacenar las claves originales o semillas (valor inicial) de un generador de números aleatorios.

2.4.3 Nombres de archivos

Las tarjetas inteligentes se utilizan siempre bajo el control de una terminal. Los nombres estándar de los archivos consisten de un elemento de datos llamado identificador de archivo de 2 bytes (FID por sus siglas en inglés). El FID del MF, es "3 F00" y está reservado para este propósito. Todos los FIDS pueden ser elegidos libremente. En la tabla 3 se muestran los nombres de archivo comúnmente usados de tarjetas inteligentes y un resumen de su función característica.

Cada archivo dedicado (DF) tiene un nombre que se añade a la FID, y se puede abordar en el árbol de archivos con este nombre complementario. Este nombre complementario se llama el nombre del DF, y por lo general incluye un identificador de la aplicación (AID). La AID consiste en un identificador de proveedor de aplicaciones registradas (RID) y un propietario para determinar la extensión de aplicación (PIX). El RID puede estar oficialmente registrado para garantizar que es único en todo el mundo. En este caso, el PIX se puede utilizar cuando sea necesario para identificar un DF específico. Esto hace que sea posible definir un nombre único para aplicaciones específicas de tarjeta inteligente, que puede ser usado para reconocer y seleccionar cada tarjeta inteligente.

Los EF previstos para guardar los datos también son FIDs asignados, similares a todos los archivos de la tarjeta inteligente. Además cada uno de los EF tiene un SFI (identificación de archivo corto), que se puede proporcionar como un parámetro de comandos de lectura o escritura para seleccionar el EF directamente

Tabla 3. Nombres de archivos de acuerdo a la norma ISO/IEC 7816-4

Tipo de dato	Nombre de archivo	Tamaño	Valor del rango
MF (Archivo maestro)	FID (Identificador de archivo)	2 bytes	'3F00´´
DF (archivo dedicado)	FID (identificador de archivo)	2 bytes	0…..´FFFF´
	DF (el nombre	1 a 16 bytes	´0…….´F……F´

Tipo de dato	Nombre de archivo	Tamaño	Valor del rango
	usualmente incluye un AID)		
	AID (RID_PIX)	5 a 16 bytes	De acuerdo a la definición de AID
EF(archivo elemental)	FID (identificador de archivo)	2 bytes	0…….´FFFF
	SFI (Identificador corto de archivo)	5 bits	1……´30´

2.4.4 Estructura de los archivos

Los archivos de datos de una tarjeta inteligente (EF) tienen estructuras internas. Esto significa que los datos almacenados en los archivos se pueden organizar de varias maneras. Como se explico en el apartado 2.4.2, cinco estructuras diferentes están disponibles, como se ilustran en la figura 2, donde cada celda representa un byte.

En la estructura transparente, se disponen los elementos de datos como una serie de bytes (cadena de bytes). Los comandos READ BINARY y UPDATE BINARY se pueden utilizar para leer o escribir los datos en esta estructura de archivos a partir de parámetros que especifican un número entero de bytes y un desplazamiento desde el inicio del archivo. Esta estructura de EF es de propósito general que se puede emplear en una amplia variedad de usos.

El tamaño máximo del archivo no se especifica, pero el rango de dirección máximo de READ BINARY y UPDATE BINARY limita a 33 023 bytes (que consiste en un máximo desplazamiento de 32 768 bytes y una longitud máxima de lectura o escritura de 255 bytes).

Además de la estructura de archivos transparente, hay tres estructuras de registros de archivos orientados. Los EF con una estructura lineal de archivo fijo se pueden utilizar para registros “dommy” de igual longitud. La estructura lineal permite archivos variables con los registros de diferentes longitudes. Si registros con diferentes longitudes deben ser almacenados en una tarjeta inteligente, la cantidad de espacio de memoria requerida será menor. Estas dos estructuras de archivos normalmente se utilizan para almacenar datos personales como direcciones o números de teléfono.
La estructura de archivos cíclica amplía la estructura de archivos lineales para incluir un puntero como índice en el registro que ha sido escrito más recientemente.

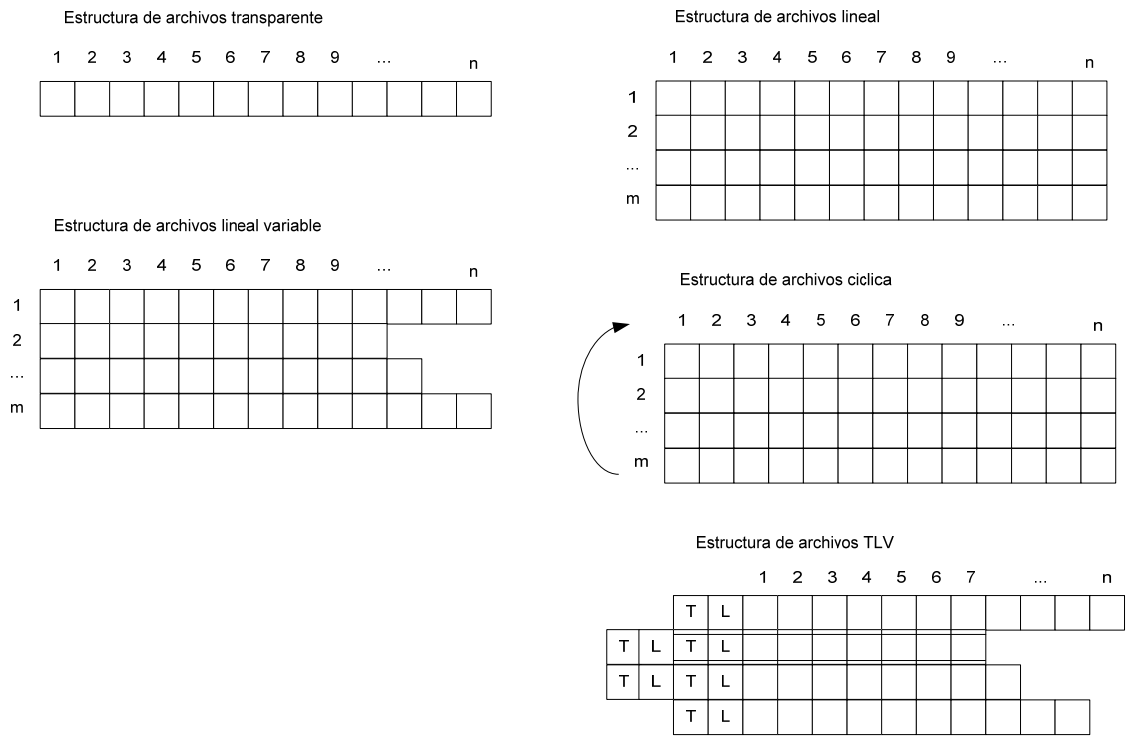


Figura 2. Estructura de archivos de datos (EF) usados en tarjetas inteligentes

Los registros orientados de los archivos pueden ser leídos y escritos utilizando el registro leído y el comando de actualización RECORD. Normalmente, sólo es posible leerlos o escribirlos completos, aunque relativamente recientemente sistemas operativos también soportan el acceso a registros parciales.

El quinto tipo de archivo permite la estructura de objetos de datos que se almacenan en una estructura TLV. En esta estructura, cada objeto de datos es identificado por la etiqueta (T) y longitud (L), elementos, que son seguidos por los datos reales o el valor (V). Esta estructura de archivos también se puede utilizar para almacenar objetos de datos anidados. Los objetos de datos pueden ser leídos y almacenados utilizando los comandos de datos GET y PUT.

La tabla 4 enumera los diferentes tipos de archivos de las tarjetas inteligentes y se resumen sus características principales.

Tabla 4. Tamaños mínimos y máximos de archivos

Estructura de Archivo	**Característica**	**Típicos tamaños de archivo y número de registros**
Transparente	Tamaño total	1-33023 bytes

Estructura de Archivo	Característica	Típicos tamaños de archivo y número de registros
Lineal	Longitud de registro Número de registros	1-255 bytes 1-254
Lineal variable	Longitud de registro Número de registros	1-255 bytes 1-254
Cíclico	Longitud de registro Número de registros	1-255 1-254
TLV	Tamaño de datos objeto Número de registros	No especificado Típicamente 255

2.4.5 Atributos de los archivos

Los archivos en las tarjetas inteligentes también pueden tener atributos diferentes, dependiendo de la operación específica del sistema. El conjunto más conocido de atributos es compartible o no compartible. Estos atributos se pueden utilizar para especificar para cada archivo si permite lectura o escritura concurrente a través de múltiples canales lógicos. Hay otros muchos posibles atributos de archivo, pero no están estandarizados.

2.4.6 Selección de archivos

El comando SELECT es utilizado para seleccionar un archivo de forma explícita. Un archivo debe siempre ser seleccionado antes de que se pueda acceder por los comandos como READ BINARY o UPDATE BINARY.

Uno de los identificadores disponibles (FID, DF Nombre) debe de ser utilizado para la selección, dependiendo del tipo de archivo (MF, DF o EF). Estos identificadores no tienen que ser únicos en el directorio y la estructura de archivos de una tarjeta inteligente. En consecuencia, las opciones de selección dependerán del archivo seleccionado.

La figura 3 ilustra los métodos de selección que se pueden utilizar en el directorio y la estructura de archivos. La opción 1 selección explicita usando un FID; opción 2 selección implícita usando un SFI; opción 3 selección usando un nombre DF; opción 4 selección usando un FID y un parámetro trayectoria.

La selección con un nombre de ruta proporciona el método de selección rápida a través de varias decisiones con un único comando. Con este método, la ruta del archivo a ser seleccionado se pasa a la tarjeta inteligente como un parámetro de comando. Esta ruta puede hacer referencia al MF o al archivo seleccionado. Ésta es la opción más sencilla de selección, y sobre todo, es la opción que requiere la menor cantidad de tiempo de transacción. El MF se puede seleccionar de una manera similar. Se puede seleccionar desde cualquier lugar en el árbol de archivos completo con un solo comando. Los cuatro comandos de uso común leer

y escribir (READ BINARY, UPDATE BINARY, READ y UPDATE) también soportan la selección de archivos durante la operación del comando (selección implícita).

Esto elimina la necesidad de utilizar el SELECT para seleccionar el archivo deseado antes de emitir el comando de lectura o escritura. Esta función de selección de archivos es llamado implícito, y es muy útil para reducir los tiempos de acceso de archivo.

2.4.7 Condiciones de acceso

De acuerdo con ISO/IEC 7816 parte 4 y 7, y Rankl [18], las condiciones de acceso asociadas con los archivos definidos en un sistema de archivos son un elemento esencial del componente del sistema operativo. En ellos se especifican las condiciones que deben cumplirse para el acceso de lectura o escritura de los archivos. Estas condiciones podrían ser, por ejemplo, éxito en el Pin, verificación o autenticación exitosa de la terminal por la tarjeta inteligente.

Dos diferentes métodos técnicos se utilizan comúnmente en tarjetas inteligentes para las condiciones de acceso: acceso basado en las condiciones de estado y acceso basado en las reglas de las condiciones. El primer método es el utilizado durante más de una década en los grandes sistemas, como los Sims, empleados en los sistemas de telecomunicaciones móviles GSM.

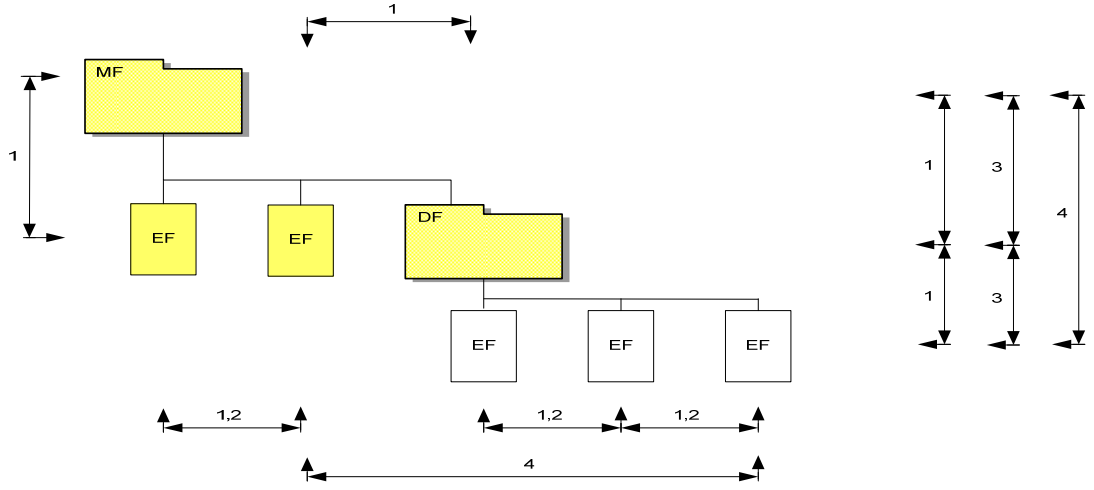


Figura 3. Métodos para la selección de archivos

2.4.7.1 Acceso basado en las condiciones de estado

En el caso de acceso basado en las condiciones de estado, cada forma de acceso (lectura y escritura) únicamente es posible si un determinado estado es alcanzado, con independencia de las formas de acceso.

Casi todos los archivos de aplicaciones de tarjetas inteligentes se pueden implementar utilizando acceso basado en las condiciones de estado. Sin embargo, sistemas operativos de un creciente número de tarjetas inteligentes soportan el método basado en reglas, que es más a futuro y significativamente más flexible.

2.4.7.2 Acceso basado en reglas de las condiciones de estado

El acceso basado en las reglas de las condiciones de estado de las tarjetas inteligentes para la asignación de todos los archivos (DF y EF) soportan las referencias a un registro de archivo que contiene reglas de acceso a conjuntos orientados. A este archivo se le asigna el nombre de la regla de acceso de referencia (EFarr), y cada referencia es compuesta por las EFarr de las FDI y un número de registro que aborda el conjunto de reglas. El FID de EFarr se puede seleccionar libremente.

Cada registro en EFarr contiene un conjunto de reglas para las diferentes formas de acceso, como de lectura y escritura. Como los archivos del directorio también pueden ser asignados a las referencias EFarr, también es posible establecer reglas para la creación y supresión de archivos. Este método también puede utilizarse de manera similar para administrar el acceso a los datos objetos.

Con el acceso basado en reglas de las condiciones de estado, es posible especificar que ciertos archivos se pueden acceder solamente a través del sistema de mensajería de seguridad (Secure Messaging). La norma ISO/IEC 7816-9 forma la base para la codificación y la funcionalidad disponible, pero siempre se deben consultar las especificaciones del sistema operativo utilizado en la tarjeta inteligente, ya que el estándar establece muchas opciones y hay grandes diferencias entre los sistemas operativos. El principio de funcionamiento del acceso basado en las reglas se ilustra en la figura 4.

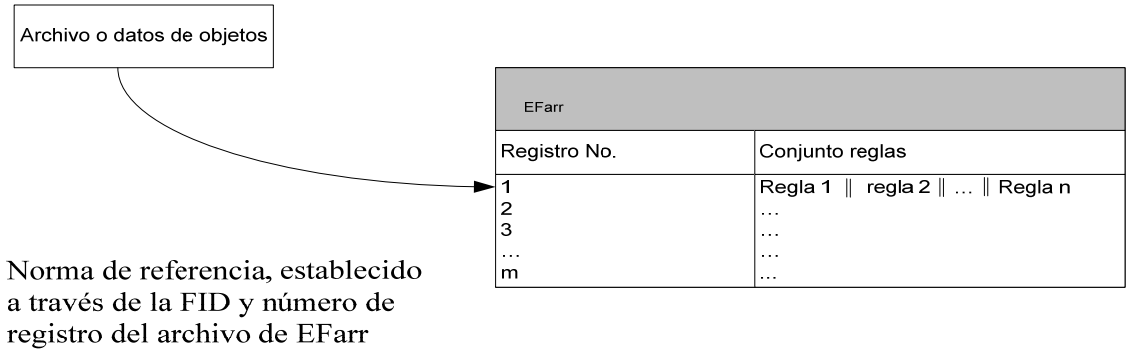


Figura 4. Principio de acceso a archivos basado en reglas

Todos los requisitos comúnmente encontrados para el acceso a los archivos y objetos de los datos en las aplicaciones de las tarjetas inteligentes se pueden implementar mediante el acceso basada en las reglas de condiciones de estado.

Aunque este método no es sencillo, es muy poderoso. Con respecto a la seguridad, podemos señalar que es esencial para garantizar que los accesos de escritura a EFarr sólo pueden ser realizadas por entidades autorizadas. De lo contrario, la seguridad completa de una aplicación puede ser pasada por alto.

2.4.7.3 Ciclo de vida del archivo

En el caso ideal, es posible crear, utilizar y eliminar archivos en un archivo de tarjetas inteligentes cada vez que así se desee. El ciclo de vida de los archivos, se ilustra en la figura 5.

Todas estas opciones están disponibles en los grandes sistemas operativos de tarjeta inteligente.
Por otro lado, los sistemas operativos simples suelen tener restricciones en este sentido. Por ejemplo, los sistemas operativos simples a menudo no permiten que los archivos se borren una vez creados o si se permite que se eliminen los archivos, la cantidad de memoria libre disponible se reducirá en varios bytes por cada paso a través del ciclo de vida descrito.
Por supuesto, estos sistemas operativos simples tienen la ventaja de que pueden funcionar en microprocesadores con poder de procesamiento significativamente menor que lo que se requiere para ejecutar un sistema operativo que soporta la gama completa de opciones del ciclo de vida de archivo. La versión más simple es totalmente adecuada para muchos programas de tarjetas inteligentes.

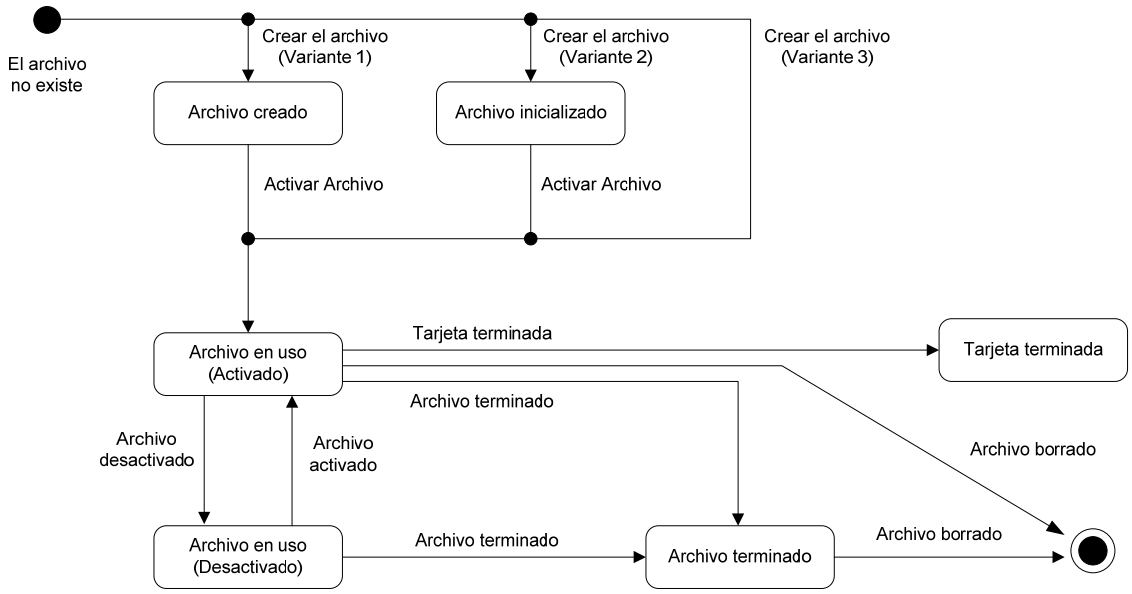


Figura 5. Estados y transiciones de estado durante el ciclo de vida de un archivo, como lo especifica ISO/IEC 7816-9

2.4.7.4 Peticiones

Aparte de la gestión de archivos, los comandos con la funcionalidad más importante en un sistema operativo de la tarjeta es lo que ofrece al mundo exterior. El número de comandos de soporte por los sistemas operativos modernos pueden fácilmente ascender cerca de los 50. Esto es totalmente adecuado para la ejecución de la mayoría de aplicaciones, incluyendo aplicaciones complicadas, sin usar comandos complementarios definidos por el usuario. De acuerdo a ISO/IEC 7816-4,-8 y -9 y como lo resume Wolfgang [18] en la tabla 5 se presenta un resumen de comandos de tarjetas inteligentes.

Con respecto a la codificación exacta de los comandos individuales, siempre hay que referirse a las especificaciones del sistema operativo utilizado por la tarjeta inteligente.

Los comandos para las operaciones de archivo SELECT INCLUDE se utiliza para seleccionar un archivo específico, READ y READ REGISTER BINARY se utilizan para leer datos de archivos que tienen diferentes estructuras. Por otra parte, UPDATE BINARY y UPDATE REGISTER son los comandos para escribir datos en los archivos. Los comandos SEARCH, SEARCH BINARY y SEARCH REGISTER pueden ser utilizados para buscar valores específicos en el directorio asociado y en la estructura de archivos EF.

Para gestionar los archivos del directorio (DF) y de los archivos de datos (EF) en

el árbol de archivos de una tarjeta inteligente se usan FILE CREATE para crear nuevos archivos, APPEND RECORD para ampliar los archivos, y DELETE FILE para borrar archivos existentes. ACTIVE FILE y DESACTIVE FILE se utilizan para activar y desactivar archivos y los comandos FILE BLOCK y FILE UNBLOCK para bloquear y desbloquear archivos. Los comandos FINISH DF y FINISH EF para bloquear permanentemente archivos, sin eliminarlos del árbol de archivos.

Comandos de datos objeto de las aplicaciones pueden ser almacenados en los objetos de datos y/o archivos, como obtener, leer y escribir los datos objetos.

El comando más conocido para funciones de seguridad COMPROBATE, se utiliza para verificar el Pin. Peticiones de un número aleatorio se realiza mediante GET CHALLENGE, una petición que se utiliza para autenticar el mundo exterior con respecto a la tarjeta inteligente se efectúa a través del comando EXTERIOR AUTHENTICATE. Así mismo, INTERIOR AUTHENTICATE puede ser utilizado para autenticar una tarjeta inteligente con respecto al resto del mundo utilizando un proceso de respuesta. La Autenticación mutua puede ser utilizada para autenticar la tarjeta inteligente y el mundo exterior una con respecto a la otra, en una sola operación. La operación de comandos de seguridad (PSO por sus siglas en inglés) se puede utilizar para invocar todas las funciones de cifrado de una tarjeta inteligente bajo el control de los parámetros proporcionados.

Tabla 5. Lista de los comandos más importantes definidos por ISO/IEC 7816-4,-8-9 y Global Platform

Función	Comando	Descripción
Archivo	SELECT	Selecciona una operación de archivo
	READ BINARY READ RECORD	Lee datos desde un archivo transparente o reorientado
	UPDATE BINARY UPDATE RECORD	Escribe datos en un archivo transparente o reorientado
	SEARCH BINARY SEARCH RECORD	Búsqueda de acuerdo a un patrón en un archivo transparente o reorientado
Gestión de archivos	CREATE FILE	Crea un archivo (DF o EF)
	APPEND RECORD	Crea un registro nuevo en un archivo orientado por registros
	ACTIVATE FILE	Desbloquea reversiblemente un

Función	Comando	Descripción
		archivo
	DEACTIVATE FILE	Bloquea reversiblemente un archivo
	TERMINATE DF/EF	Bloque permanentemente un archivo (DF o EF)
	DELETE FILE	Borra un archivo (DF o EF)
Datos objetos	GET DATA	Lee datos objetos TLV
	PUT DATA	Escribe datos objetos TLV
Seguridad	VERIFY	Verifica la transferencia de datos
	GET CHALLENGE	Requiere un número aleatorio (ejemplo: para una posterior externa)
	INTERNAL AUTHENTICATE	Autenticación unilateral de una tarjeta por el mundo externo
	EXTERNAL AUTHENTICATE	Autenticación unilateral del mundo exterior por una tarjeta
	MUTUAL AUTHENTICATION	Autenticación mutua de la tarjeta y el mundo exterior
	PERFORM SECURITY OPERATION	Ejecuta un algoritmo criptográfico en la tarjeta
	MANAGE SECURITY ENVIRONMENT	Maneja parámetros de comandos de seguridad
Administración de código de programas	LOAD	Carga una aplicación basada en código
	INSTALL	Instala una aplicación basada en código
	PUT KEY	Carga una llave para una aplicación basada en código
	SET STATUS	Escribe información del estado del ciclo de vida de la tarjeta o de una aplicación
	GET STATUS	Lee el estado de la información acerca del dominio de seguridad, carga de archivos o aplicaciones

Función	Comando	Descripción
	DELETE	Borra un objeto
Transmisión de datos	GET RESPONSE	Requiere datos para protocolos de transmisión T=0 desde la tarjeta

En el nivel de ejecución máximo, puede implicar una suma de comprobación de cifrado (CCS) o un código de autenticación de mensajes (MAC), una digital firma o un valor hash. Además, la PSO se puede utilizar para verificar una firma digital o certificado para cifrar o descifrar.

El comando SECURE (MSE) se utiliza para gestionar todos los parámetros de seguridad de una tarjeta inteligente. Puede ser utilizado para configurar todos los parámetros necesarios para la mensajería de seguridad y las funciones criptográficas invocadas por el comando PERFORM de operación de seguridad.

Para la gestión de tarjetas de código inteligente que pueden descargar código de programas ejecutables, se necesitan varios comandos. A diferencia de todos los demás comandos, los comandos para este fin no están estandarizados por ISO/ IEC, sino que se definen por la especificación generada por la organización Global Platform.

Finalmente podemos decir que en este apartado, se han revisado los conceptos fundamentales de los sistemas operativos de tarjetas inteligentes, los cuales proporcionan los mecanismos para la comunicación, transferencia de datos y mensajes, entre la tarjeta y el mundo exterior representado por el SGTI.

2.5 Ciclo de vida de tarjetas inteligentes y aplicaciones

2.5.1 Diagrama de estados del ciclo de vida de tarjetas y sus aplicaciones

Una de las principales características de las tarjetas inteligentes y cuya funcionalidad es lo que le otorga un gran potencial en el manejo transaccional y reutilización de la tarjeta a través de aplicaciones que se pueden cargar o actualizar en etapa de postemisión por parte del titular de la misma, es el ciclo de vida de la tarjeta y las aplicaciones contenidas en ella.

Parte de la funcionalidad más importante de los sistemas operativos de las tarjetas inteligentes, en la interfaz que ocurre entre éste y el SGTI, es el tratamiento de la información y su actualización de los diferentes estados y las transiciones de las etapas que conforman el ciclo de vida.

Para abordar los fundamentos de la funcionalidad de esta característica de las tarjetas inteligentes se describen los conceptos de máquina de estado.

De acuerdo con Hopcroft, Motwani y Ullman [37], se conoce como teoría de autómatas el estudio de las máquinas o dispositivos abstractos con capacidad de computación, donde se destaca que una de sus principales aplicaciones consiste en el desarrollo de software para comprobar la corrección de cualquier tipo de sistemas que tengan un número finito de estados diferentes, como los protocolos de comunicación o los protocolos para el intercambio seguro de información.

Siguiendo con Hopcroft [37], se refiere a un autómata finito como un sistema o componentes del mismo, de los que se puede decir en todo momento que están en cierto estado, entre un número finito de ellos. El objetivo de un estado es recordar la parte significativa de la historia del sistema.

Abundando un autómata finito determinista, es aquel que siempre está en un solo estado después de leer cualquier secuencia de entradas. Donde el término determinista hace referencia al hecho, de que para cada entrada, existe un único estado al que el autómata puede llegar partiendo del estado actual. En cambio los autómatas no deterministas pueden estar en varios estados al mismo tiempo.

Para nuestro caso, se centra el estudio en los estados finitos deterministas. El valor de estos conceptos se centra en aplicarlo a los diferentes estados que guardan los archivos de una tarjeta inteligente, que como veíamos en el apartado precedente están regulados por el estándar ISO/IEC 7816-9, y que son: creado, inicializado, activado, desactivado y terminado.

Estos conceptos son aplicados en apartados siguientes a tarjetas y aplicaciones.

El apoyo con gráficos de redes puede ser muy efectivo para visualizar máquinas de estado. Estos no sólo son útiles para el modelado de máquinas de estado, también pueden utilizarse para investigar algunas propiedades de los sistemas que describen. Los objetivos son identificar cualquier bloqueo que pueda ocurrir en el proceso y garantizar el procesamiento de comandos correcto.

El objetivo de este apartado es proporcionar una introducción a los diagramas de estado, que se utilizan para describir las aplicaciones de tarjetas inteligentes, y una explicación general de cómo interpretarlos.

De acuerdo con Silva Bijit [R27]:

- Un diagrama de estados puede emplearse para describir la conducta de un programa que cambia entre estados, conducido por eventos externos y realizando acciones al efectuar transiciones de un estado a otro
- Un estado es una condición del sistema que persiste durante un tiempo significativo de tiempo
- Un evento es un mensaje hacia la máquina de estados producido por una entrada externa

- Una transición es un cambio de un estado a otro, disparada generalmente por un evento
- Una acción es una tarea que puede tomar lugar durante una transición, cuando se entra o sale de un estado
- Una interrupción es un evento que puede disparar una transición
- En un sistema embebido se modela la computación como una secuencia de transiciones entre un conjunto de estados. En cada estado, la llegada de eventos (o entradas) pueden cambiar el estado y posiblemente generar una acción (o salida)

Retomando a Wolfgang [17], un diagrama de estado es un gráfico que representa un conjunto de estados y las interrelaciones de ellos. Los estados se muestran como nodos, y sus relaciones se muestran como líneas. Si una línea indica una dirección, significa que tiene una punta de flecha en un extremo, se le llama una "dirección línea " y la gráfica es un grafo dirigido. La flecha indica la dirección en que la transición de un estado puede tomar lugar. La ubicación real de los nodos y líneas en el gráfico no desempeña ningún papel en la interpretación de la figura 6.

Una secuencia de nodos conectados por líneas se denomina ruta de acceso. Si el primer nodo y el último son los mismos y no hay más de un nodo, se llama la ruta de un bucle.

Ésta es solamente una parte muy pequeña de la teoría de grafos, pero es básicamente todo lo que necesitamos para poder describir los estados y sus máquinas de estado asociados en las solicitudes que se realizan en las tarjetas inteligentes.

Una ventaja adicional de las tarjetas de microprocesador en comparación con las tarjetas de memoria simple es que las secuencias de comandos se pueden especificar por adelantado. Así, es posible especificar con precisión todos los comandos en términos de sus parámetros y la secuencia. En combinación con la orientación de objetos para la autorización del acceso a los archivos, proporciona una protección adicional contra el acceso no autorizado

Sin embargo, las posibilidades que ofrecen las tarjetas inteligentes en este sentido varían mucho. El funcionamiento de sistemas simples generalmente no pueden manejar las máquinas de estado, mientras que con los sistemas operativos modernos es posible definir la aplicación de máquinas de estados específicos que trabajan con los parámetros de los comandos.

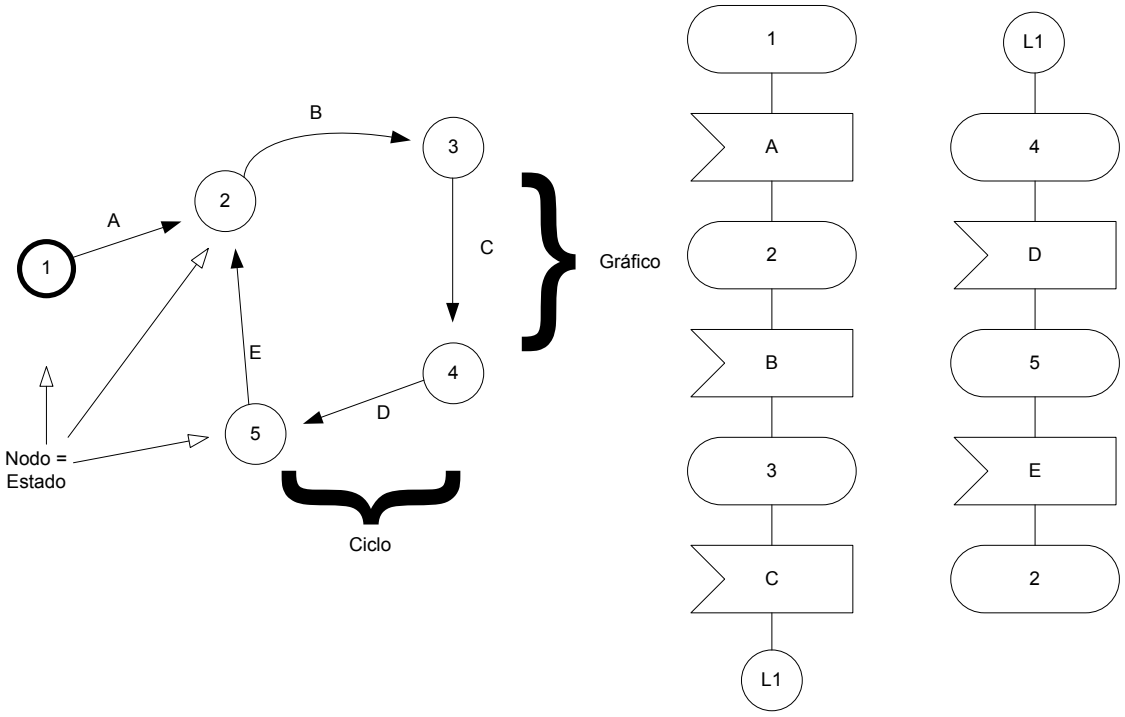


Figura 6. Dos diferentes representaciones de diagramas de estado

Un ejemplo típico de una máquina de estados simple es proporcionado por los dos comandos necesarios para autenticar una terminal. El primer comando solicita a la tarjeta un número aleatorio. Esto activa una máquina de estado que sólo acepta un comando de autenticación como el siguiente comando. Si la tarjeta recibe este comando, el proceso se completa y cualquier otro tipo de mando se admite.

Si la tarjeta recibe cualquier otro comando diferente a un comando de autenticación, la máquina de estados genera un mensaje de error y el proceso se concluye. La secuencia de comandos debe entonces ser reiniciada desde el principio.

Estas máquinas de estados simples tienen varias ventajas importantes en las tarjetas inteligentes. Puesto que son limitados a muy pocos comandos en una secuencia rígidamente definidas, que requiere poco espacio de memoria para la ejecución del programa. En muchas aplicaciones, es suficiente con proteger el contenido del archivo usando mecanismos orientados de acceso, sin ninguna imposición de otras restricciones sobre las secuencias de comandos.

Sólo algunos procedimientos, como la autenticación, deben seguir las secuencias prescritas. Esto puede llevarse a cabo con muy poca memoria utilizando máquinas de estado simple. Estas máquinas de estado simple se pueden extender para verificar todos los comandos, junto con todos sus parámetros,

dentro de un gráfico definido antes de ser ejecutados. Dependiendo de cómo la máquina de estados se construye, en determinadas condiciones es posible prescindir de objetos orientados de protección de archivos, ya que la máquina de estado puede llevar a cabo todos los controles necesarios antes de que un comando sea realmente ejecutado. Un error en el diagrama de estado puede tener consecuencias fatales para la seguridad del sistema. Como es muy difícil verificar la completa ausencia de errores en los diagramas de estado de las máquinas de estado complejo, la protección de archivos de acceso todavía se utiliza en la práctica. Describir correctamente todos los procesos y los comandos presentes en una tarjeta inteligente es muy lento, por lo que a menudo es necesario hacer esto empíricamente.

Ahora que están descritas las ventajas de las máquinas de estado, podemos también mencionar sus inconvenientes.
La aplicación de una máquina de estados con la capacidad requerida es costosa en términos de tiempo de diseño y de programación posterior. Cuando una máquina de estado es controlada y su representación gráfica es almacenada, una considerable cantidad de memoria se necesita para cargar una máquina de estados, ya que el gráfico debe ser almacenado en la memoria, además de la situación real de máquina. La cantidad de espacio de memoria, naturalmente, depende de la complejidad de la gráfica que se va a ejecutar. La cantidad de información contenida en un gráfico con muchos estados, y el correspondiente número de transiciones pueden ser muy grandes en relación con la capacidad de memoria típica de la tarjeta inteligente.
Las máquinas de estado para las tarjetas inteligentes son abordadas por la norma ISO/IEC 7816-9. En ella se especifican descriptores de control de acceso (CLSA), que definen los comandos que permiten un determinado estado, en conjunto con sus parámetros asociados. Un sistema operativo de tarjetas inteligentes puede controlar las maquinas de estado codificadas utilizando estos CLSA.

2.5.2 Ciclo de vida y estados de las tarjetas inteligentes

En este apartado se revisa el ciclo de vida de las tarjetas inteligentes, atributo mediante el cual se posibilita la rastreabilidad de los eventos que se llevan a cabo desde que se fabrica el microprocesador hasta que termina su vida útil.

La funcionalidad de carga, descarga o actualizaciones de aplicaciones en las tarjetas está controlada por los diferentes estados en que puede estar la tarjeta, así como también las facilidades de poder recuperar una tarjeta perdida a imagen del último estado registrado.

El ciclo de vida de las tarjetas está conformado por diferentes estados y sus transiciones, lo cual permite la rastreabilidad a lo largo de la ejecución de diferentes eventos.

La norma ISO/IEC que establece el ciclo de vida de la tarjeta y las aplicaciones que residen en ella es la ISO/IEC 10202, donde los diferentes estados que toma cada ciclo son administrados mediante el sistema operativo ligado a un SGTI.

Aunque esta norma ha sido retirada del catálogo de ISO/IEC, la norma equivalente europea EN 30202-1 está disponible, además de que es un referente válido en la industria.

Una tarjeta inteligente consta básicamente de dos componentes completamente diferentes. El primer componente es el cuerpo de la tarjeta, su impresión, sus características de seguridad gráfica física y posiblemente, una banda magnética. El segundo componente, que es lo que hace que el cuerpo de la tarjeta sea una tarjeta inteligente, es el chip.

El proceso de fabricación depende en gran medida de otros elementos de la tarjeta, tales como el material utilizado para el cuerpo de la tarjeta, los métodos utilizados para la aplicación de texto y las características de seguridad gráfica.

Además del proceso de fabricación, el ciclo de vida de una tarjeta inteligente depende de las aplicaciones en que se utiliza. Una tarjeta inteligente para el sistema de telecomunicaciones móviles GSM, tiene una trayectoria muy diferente después de la fabricación, que una tarjeta financiera que contenga un chip.

La norma ISO 10202-1 define el ciclo de vida de la tarjeta, que es igualmente válido para todos los métodos de fabricación y una amplia variedad de aplicaciones. Esta norma está orientada hacia las aplicaciones de transacciones financieras y la tecnología de la información utilizada en estas aplicaciones, en lugar de la producción de tarjetas y chips. Sin embargo, representa un intento bastante exitoso para proporcionar una descripción estructurada de la historia de vida de las tarjetas inteligentes. Ésta es la razón por la que se utiliza en esta tesis como la base para describir el ciclo de vida de la tarjeta inteligente.

De acuerdo con la norma ISO 10202-1, la vida de una tarjeta se divide en cinco fases, que están interconectadas con precisión por transiciones específicas, estás se presentan en la figura 7 y se describen en la tabla 6.

La madurez de la industria se refleja en que la mayoría de las plantas y entidades empresariales que participan en la cadena de producción tienen implementados sistemas de gestión de la calidad bajo la norma ISO 9001:2008 y sistemas de gestión de la seguridad de la información bajo la norma ISO/IEC 27001.

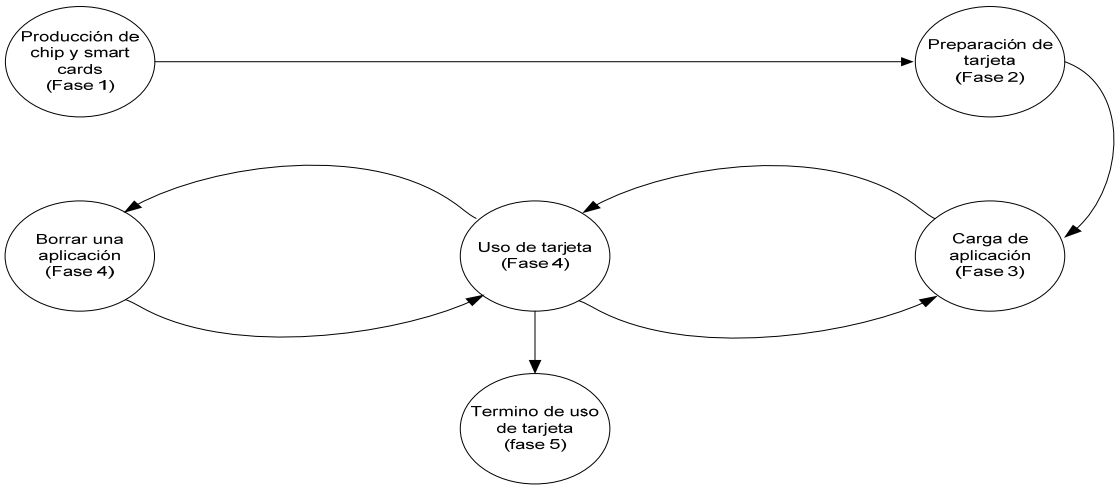


Figura 7. El ciclo de vida de una tarjeta inteligente

Tabla 6. Fases del ciclo de vida de acuerdo a la norma ISO/IEC 10202-1

Fase	**Descripción de la Fase**	**Actividades típicas**
1a	Producción del chip y la tarjeta inteligente	Diseño del chip Generación del sistema operativo de la tarjeta Fabricación del chip y módulos de hardware Producción del cuerpo de la tarjeta Embebido del chip en el cuerpo de la tarjeta
2a	Preparación de la tarjeta	Complemento del sistema operativo de la tarjeta
3a	Preparación de las aplicaciones	Inicialización de aplicaciones Personalización de aplicaciones, visual y eléctrica
4a	Uso de la tarjeta	Activación de aplicaciones Desactivación de aplicaciones
5a	Terminación del uso de la tarjeta	Desactivación de aplicaciones Desactivación de la tarjeta

En este ambiente de trabajo los pasos de producción, están inscritos en los procesos de aseguramiento de la calidad. Las tarjetas inteligentes se utilizan normalmente en las aplicaciones en las que la seguridad es un requerimiento, la trazabilidad del proceso de fabricación se debe de garantizar de acuerdo con la aplicación de la familia de normas ISO 9001:2008. Esto significa que todos los pasos de la producción deben estar conectados utilizando lotes y números de chip. Debe ser posible reconstruir los pasos de producción para cada una de las

tarjetas inteligentes de manera individual, en cualquier momento después de que haya sido fabricada.

Esto hace que sea más fácil analizar la causa de los defectos de fabricación que puedan presentarse. Dado que cada chip individual tiene un número único, no hay dos microprocesadores que sean idénticos de raíz en el proceso de fabricación, lo que hace que sea relativamente fácil de implementar la trazabilidad sobre la base del número del chip. La trazabilidad de fabricación puede ser llevada a cabo, ya sea mediante el almacenamiento de la información pertinente en una base de datos de fabricación o en el propio chip. La norma ISO 10202-1 recomienda almacenar los datos de fabricación en los chips, lo que representa ciertas ventajas en comparación con el almacenamiento de los datos en una base de datos. Si los datos son almacenados en los chips, esto va en detrimento de valioso espacio en la EEPROM del microprocesador.

La tabla 7, muestra los datos típicos durante las tres primeras fases del ciclo de vida

Tabla 7. Datos de manufactura almacenados en chips

Fase del ciclo de vida de la tarjeta inteligente	Datos típicos de fabricación
1ª Fase Producción del chip y tarjeta inteligente	ID del fabricante del chip ID de la línea de fabricación Número único de chip Tipo de chip ID del módulo embebedor Fecha y hora del embebido del chip en el módulo
2ª Fase Preparación de la tarjeta	ID del inicializador ID de la máquina terminadora Fecha y hora de inicialización
3a Fase Carga de aplicaciones	ID del personalizador ID de la máquina terminadora Fecha y hora de personalización

De acuerdo a la norma ISO/IEC 10202 [W15] y al análisis que realiza Wolfgang [17] las fases del ciclo de vida quedan expresadas como sigue:

2.5.2.1 Primera fase del ciclo de vida

La primera fase del ciclo de vida estándar ISO 10202-1 se puede subdividir en dos partes. La primera de ellas abarca la generación del sistema operativo de la tarjeta inteligente y el proceso de fabricación de los semiconductores para el

microprocesador, mientras que la segunda parte abarca toda la tecnología para la producción del cuerpo de la tarjeta.

La funcionalidad del SGTI, para esta fase del ciclo de vida, es el de registrar los perfiles de las tarjetas y de las aplicaciones primarias contenidas en ellas, esto a la postre forma parte del portafolio de tarjetas y aplicaciones.

Generación del sistema operativo y la producción del chip

Los sistemas operativos y el software para microprocesadores de tarjetas inteligentes son complejos, sin embargo, no debemos pasar por alto el hecho de que una parte significativa de la base técnica para la seguridad del ciclo de vida de la tarjeta se establece desde la fabricación del chip.

No importa qué funcionalidad tenga el sistema operativo y cuántos elementos criptográficos se utilizan para la protección, ambos serían de poca utilidad si los datos secretos se pueden leer en el chip, debido a un error en el diseño o fabricación del chip. Los chips semiconductores son generalmente producidos en las instalaciones protegidas con acceso restringido. Esto es importante con respecto a la seguridad, ya que es la única manera de garantizar que no contengan caballos de Troya en su software durante la fabricación del chip. La figura 8 presenta el flujo para la producción de los chips.

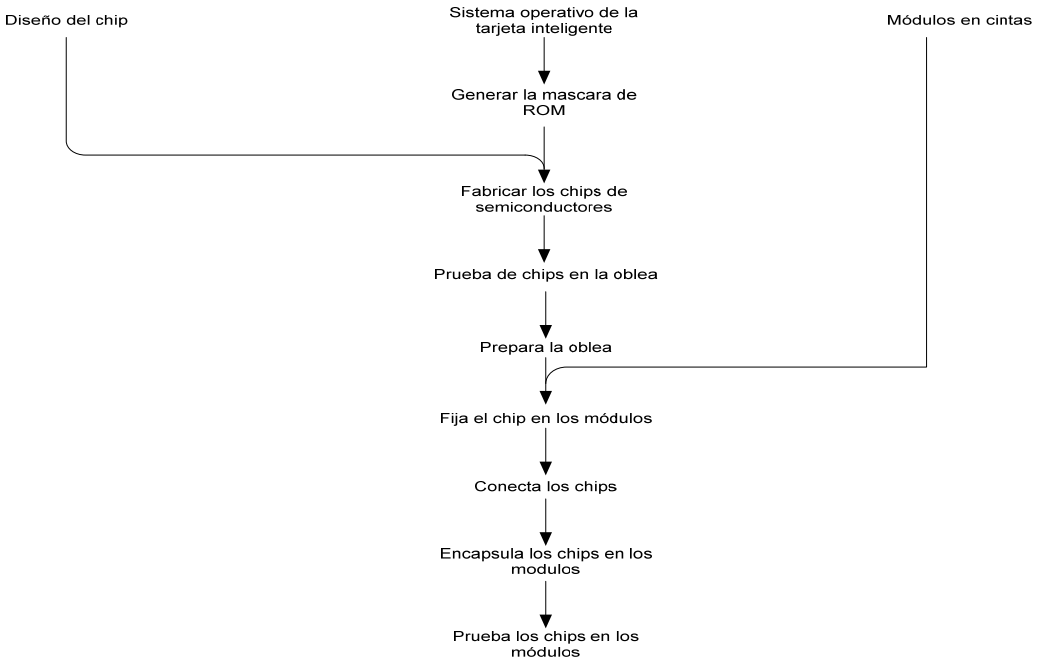


Figura 8. La produccion de chips y módulos

Diseño de chips

La estructura geométrica de un chip de memoria o un microcircuito de tarjeta debe ser cuadrado o casi cuadrado como sea posible, ya que minimiza el riesgo de que el chip se rompa por los esfuerzos que surgen cuando la tarjeta está doblada. La protección completa del chip contra las tensiones de flexión en principio son técnicamente posibles con un módulo extremadamente rígido, pero esto no es deseable en la práctica. Este módulo dura el tiempo necesario hasta que el cuerpo de la tarjeta se desgaste, debido a los esfuerzos alternados de flexión a la que la tarjeta es recurrentemente expuesta. Los componentes semiconductores que se utilizan en el chip, como el coprocesador numérico y el CPU, son normalmente componentes estándares de la industria que tienen modificaciones técnicas para proporcionar mayores y mejores niveles de seguridad.

Elementos semiconductores son tomados de la experiencia de la industria automotriz, que se suelen utilizar para este propósito, ya que deben estar diseñados para satisfacer los requisitos medioambientales y de confiabilidad. Sin embargo, dichos componentes deben ser modificados según sea necesario para adaptarse plenamente a los requisitos impuestos a la seguridad de los microprocesadores de la tarjeta inteligente.

En el proceso de diseño de los chips, el primer paso después de establecer la especificación funcional es generar una arquitectura general del chip, con un diagrama de bloques del circuito y un esbozo del diseño del microprocesador futuro. Después de este paso, se refina el diagrama de bloques general en 3 pasos. La lógica de los bloques, el nivel de funciones de las puertas de transistores y, finalmente, las estructuras geométricas de las máscaras de la presentación individual. Cada paso es acompañado por procesos de simulación y amplias pruebas de circuitos. Éste es un proceso complejo, compuesto de muchos pasos individuales, y es necesaria bastante experiencia para llegar a la disposición óptima de los elementos del chip. Al final de este proceso, los chips de muestra se producen en una línea de producción de la planta de fabricación. Estos son los dispositivos de primera referencia, que son medidos con precisión. Una evaluación de la seguridad se realiza en paralelo, aunque la evaluación no se puede completar antes de que se hayan producido los primeros chips.

El proceso de diseño de un chip puede tomar varios de meses antes de que el funcionamiento completo cumpla todos los requisitos necesarios para la producción masiva. El hecho de que se tome tanto tiempo y esfuerzo para diseñar un chip es la razón por la cual el intervalo entre sucesivas generaciones de microprocesadores de tarjetas inteligentes sea de dos a tres años. Debido al alto costo de realizar cambios significativos en un chip existente, las modificaciones más sustanciales son predominantemente el "reducir" el chip, con el fin de aprovechar mejor el área de la oblea, y hacer menores mejoras o ampliaciones en el hardware.

Sistemas operativos de tarjeta inteligente

En concordancia con el apartado 4.2, el software para sistemas operativos de tarjeta inteligente y aplicaciones basadas en ellos son escritos utilizando el lenguaje ensamblador o C, debido a la pequeña capacidad de memoria de los microprocesadores. El uso de estos lenguajes, que están relativamente cerca del nivel de hardware, tiende naturalmente a prolongar la duración de todo el proceso de desarrollo del software, y por lo tanto aumenta significativamente su costo.

Las pruebas para el software, la mayoría de los cuales se encuentra en la ROM del microprocesador, es muy completa y exhaustiva, ya que es casi imposible de corregir cualquier error residual de este software después de que los chips están manufacturados, la producción de chips siempre implica la generación de las máscaras de ROM, que representan, esencialmente, el software que más tarde se encuentra en la ROM del microprocesador, donde no puede ser modificado posteriormente. Si un error del software, se detecta en las etapas siguientes de producción, únicamente puede ser corregido mediante la repetición de todos los pasos anteriores.

Con el fin de hacer el mejor uso posible del espacio de memoria disponible en el microprocesador, el código de los programas debe de ser adaptado al tipo específico de chip que se utiliza. Portar el software a otro tipo de chip, sólo es posible con mucho esfuerzo y gastos adicionales.

Esto se puede reducir significativamente si es posible reutilizar el código de programas que ya están disponibles (en forma de bibliotecas de software). Una vez que el desarrollo de la máscara de ROM está completado, se puede entregar formalmente al fabricante de semiconductores.

Máscaras y fabricación de los chips semiconductores

Después de que el software se recibe en una EEPROM, en un medio magnético o por medio de telecomunicaciones de datos, el fabricante de los semiconductores genera una máscara de presentación para la ROM del microprocesador. Esta máscara, que contiene el código del programa, se llama por los diseñadores de sistemas operativos “la máscara del ROM", o, a menudo simplemente "la máscara".

2.5.2.2 Segunda fase del ciclo de vida

De acuerdo con la norma ISO 10202-1, la segunda fase del ciclo de vida de la tarjeta inteligente describe la carga de todos los datos que no son específicos de las tarjetas, así como la implantación de los chips en el cuerpo de la tarjeta preparada. La segunda y tercera fases son frecuentemente llevadas a cabo por una sola empresa, aunque en estas empresas, las dos fases son normalmente

separadas por completo, tanto organizativamente como físicamente, por razones de la seguridad.

Un sistema de información para la planificación y el control de la producción, el cual en algunas organizaciones tiene una interfaz con el SGTI, se utiliza frecuentemente para coordinar estos procesos de producción. Las diversas máquinas de acabado obtienen sus datos de este sistema, y en paralelo, el informe sobre la situación actual de procesamiento a una estación de control central.

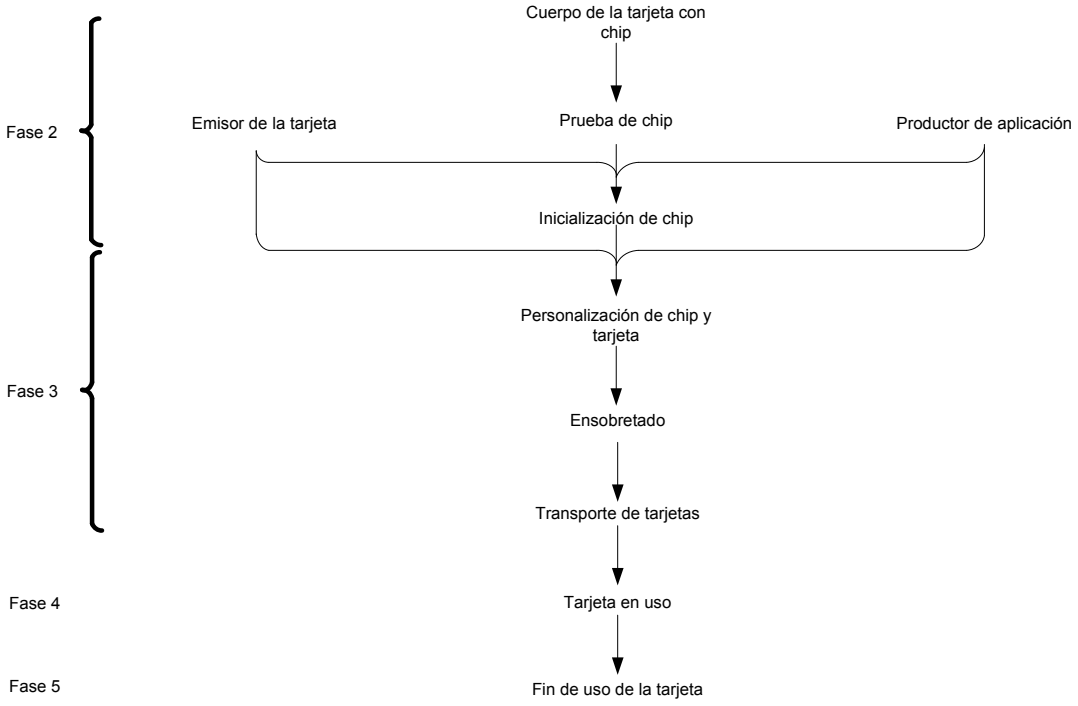


Figura 9. Fases, segunda a la quinta del ciclo de vida de la tarjeta inteligente

Adicionalmente a la funcionalidad referida en el párrafo anterior, el SGTI en esta fase del ciclo de vida deberá de estar preparado para registrar los datos asociados a las características del chip, máscara y datos particulares de la producción, los que se vinculan a los catálogos de los perfiles de tarjetas, sistemas operativos y chips.

La figura 9 muestra las actividades principales que se desarrollan de la segunda a la quinta fase.

Transferencia de datos

El emisor de la tarjeta o el proveedor de la aplicación, proporciona para la personalización de la tarjeta todos los datos relacionados con su aplicación. Esto incluye información como el nombre de la aplicación, la estructura del árbol de archivos, los archivos y las estructuras de los mismos. Esta información es cargada en las tarjetas cuando son inicializadas. Además, el personalizador proporciona también los datos específicos según las necesidades del cliente y del sistema, tales como las llaves secretas de las tarjetas, y los nombres y direcciones de los titulares de tarjetas. Esta información es transferida mediante medios magnéticos, o por medio de telecomunicaciones de datos.
Los datos de personalización son siempre sensibles con respecto a la seguridad, lo que significa que la ruta de transporte y la transferencia de datos deben ser protegidas adecuadamente. Por consiguiente, los datos son cifrados. Las llaves asociadas de descifrado son transportados a la personalizadora a través de una vía diferente a la de datos.

Esto significa que los datos de personalización no tienen ningún valor si se pierden, ya que no es posible descifrar sin la llave.
Los conjuntos de datos para cada una de las tarjetas individuales se generan en los módulos de seguridad de los equipos de acabado.

2.5.2.3 Tercera fase del ciclo de vida

La tercera fase del ciclo de vida abarca principalmente la presentación visual y eléctrica de la personalización de la tarjeta inteligente. Al igual que con la segunda fase, se produce normalmente en un entorno de producción automatizada para procesar un gran número de tarjetas.

Generación de datos secretos de las tarjetas

Como regla general, los datos individuales para la personalización, son proporcionados por el emisor de la tarjeta en un medio de almacenamiento de datos, base de datos o a través de las telecomunicaciones. Sin embargo, un método especial se utiliza a menudo para proporcionar datos secretos, como pines y las llaves, ya que dichos datos deben mantenerse en secreto en todas las circunstancias y únicamente pueden ser generados en entornos de alta seguridad.

Hay cuatro métodos que se utilizan en la práctica de Pin.

La opción más sencilla es la de generar un Pin trivial, y que posteriormente el titular de la tarjeta debe cambiar a un Pin de su elección la primera vez que la tarjeta se usa (antes de utilizar la tarjeta para una transacción válida). Sin embargo, por diversas razones este método no puede aplicarse en todos los

sistemas, aunque tiene la ventaja de no requerir la impresión y envío de cartas a usuarios con el Pin.

Una opción algo más elaborada para la generación del Pin por el emisor de la tarjeta, es utilizar un generador de números aleatorios, seguida de la transferencia segura de los códigos Pin al equipo personalizador de tarjetas. Este último escribe el Pin de las tarjetas a ser personalizadas utilizando el mecanismo de seguridad establecido y genera las cartas asociadas al Pin.

Una variación de esta opción es generar el Pin en las tarjetas, seguido por la transferencia segura de los códigos Pin a los equipos de personalización para el procesamiento posterior.

La tercera posibilidad es la generación del Pin al azar por el equipo personalizador de tarjetas. Estos pines, que se generan en un entorno seguro, se escriben en los campos de datos apropiados en las tarjetas inteligentes, como en las opciones anteriores. El emisor de la tarjeta debe tener el Pin que se genera de esta forma, y lo puede proporcionar de una manera segura. De lo contrario, generalmente no es necesario almacenar los pines generados en cualquier lugar, excepto en las tarjetas inteligentes.

Otra manera de generar el Pin es utilizar un algoritmo, que puede ser un algoritmo criptográfico, para calcular el Pin para una tarjeta especifica, utilizando datos que figuran en las cartas emitidas para los usuarios y una llave maestra. El inconveniente de este método es que la llave maestra y (en algunos casos), el algoritmo debe mantenerse secreto.

Transferencia de datos a la tarjeta inteligente

Hay dos métodos fundamentalmente diferentes que se pueden utilizar para almacenar los datos de inicialización en la memoria del microprocesador. El primer método, pretende evitar el direccionamiento físico directo de la memoria, el cual utiliza las direcciones lógicas en el microprocesador para la inicialización y la personalización en la medida de lo posible. Desde una perspectiva teórica, éste es el método preferido, ya que evita la necesidad de utilizar direcciones físicas fuera de la tarjeta inteligente.

Esto elimina de forma automática muchas fuentes potenciales de errores, dentro de ciertos límites, también hace que la carga de datos en la tarjeta inteligente sea independiente del tipo de microprocesador presente en la tarjeta inteligente. El inconveniente de este enfoque es que aumenta significativamente el tiempo necesario para la inicialización y personalización, y en particular en el caso de la producción masiva, el tiempo es un factor muy crítico. En consecuencia, hay un segundo método que se utiliza en la práctica para cargar datos en tarjetas inteligentes, que consiste en escribir los datos de inicialización directamente a la memoria del microprocesador utilizando de manera específica en el exterior las

direcciones físicas. Esto reduce significativamente la cantidad de tiempo requerido en comparación con un método basado en las direcciones lógicas. En contra parte, con este enfoque es necesario trabajar con direcciones físicas externas a la tarjeta, que lleva los correspondientes inconvenientes con respecto a la susceptibilidad a errores.

En la práctica, el método utilizado se determina generalmente caso por caso. Si el número de tarjetas inteligentes producido es suficientemente grande, el mayor costo del software para el equipo de inicialización y pruebas más complicadas puede ser justificado.

Para escribir los datos directamente en las direcciones físicas, los datos deben estar convenientemente preparados con antelación. Una manera de hacer esto es imitar el funcionamiento del sistema completo de gestión de archivos del sistema de tarjetas inteligentes en forma de una simulación. Un programa de conversión puede ser utilizado para cargar los datos que se escriben en el archivo codificado adecuadamente por los encargados de la simulación y les proporcionan sus cabeceras de archivo asociado.

Después de esto, todo lo que se necesita es reubicar los archivos construidos de esta manera a la dirección correcta en la memoria. Naturalmente, todo el proceso, debe realizarse sin errores y de una manera que se equipare con el sistema operativo en cuestión. Después de esto, los datos se pueden leer en la simulación y directamente escribir en las direcciones físicas de memoria en la tarjeta inteligente, utilizando los comandos habituales.

El método práctico utilizado es mucho más simple. Una tarjeta inteligente contiene una rutina en un espacio no utilizado en el área de memoria, se inicializa por primera vez utilizando el comando de gestión de archivos, que utiliza direcciones lógicas. La memoria se inicializa para dar lectura mediante la rutina de descarga, y los datos así obtenidos son escritos en la dirección física de la tarjeta inteligente a ser inicializada. Esto permite que los tiempos de la inicialización de la personalización se reduzcan hasta en un 30%. Su principal ventaja es que es simple y robusto, y el único aspecto crítico es que la tarjeta inteligente contiene la rutina de descarga y nunca debe ser permitido salir de la planta procesadora.

Si la tarjeta inteligente fue totalmente personalizada, el espacio que contiene la rutina podría utilizarse para leer todos los datos secretos. En consecuencia, este mecanismo no es adecuado para evitar que se emplee indebidamente la lectura de la memoria como el resultado de un intercambio o un ataque.

Personalización

El siguiente paso en la producción de una tarjeta inteligente que está lista para ser enviada al usuario, es la personalización. En un sentido más general, la personalización es cargar todos los datos asignados de una persona en particular

en la tarjeta inteligente. Esto podría ser un nombre y dirección, por ejemplo, pero también podrían ser las llaves específicas de la tarjeta.

Una distinción básica entre la personalización visual y eléctrica es el estampado, así como el texto o imágenes aplicadas a la tarjeta mediante grabado por láser, constituyen la parte visual de la personalización. La parte eléctrica consiste en cargar los datos personales en el microprocesador y escribir datos en la banda magnética. El tiempo de procesamiento para la personalización visual depende en gran medida de las características específicas y no puede ser general, la personalización eléctrica generalmente toma entre 5 y 20 segundos, dependiendo de la cantidad de datos.

El estampado de los nombres de características similares de información es realizado por un equipo que golpea la placa de metal en contra de la parte trasera de la tarjeta a gran velocidad y con una fuerza considerable. Dado que éste es un procedimiento relativamente simple, pero que es muy fuerte y produce una gran cantidad de vibraciones, las máquinas de estampado por lo general están separadas.

2.5.2.4 Cuarta fase del ciclo de vida

La cuarta fase del ciclo de vida de una tarjeta inteligente es bien conocida por los titulares y usuarios de la tarjeta con base en la experiencia diaria con sus propias tarjetas, ya que corresponde a la fase en que son portadas por los titulares y actualizadas según los requerimientos del cliente o del emisor. Las nuevas aplicaciones se pueden descargar o activar, y las aplicaciones ya presentes en la tarjeta pueden ser desactivadas si es necesario.

Esta fase del ciclo de vida, técnicamente es la que involucra más funcionalidades del sistema operativo de la tarjeta, puesto que las funciones más importantes se dan en el proceso conocido como postemisión.

En este proceso las aplicaciones y datos son actualizados, tarea que es totalmente realizada por el sistema operativo de la tarjeta con complemento funcional de otros componentes, como son los dispositivos terminales y sistemas de administración de transacciones electrónicas.

El rol del SGTI en esta fase del ciclo de vida, es mantener actualizados todos los movimientos resultantes de los procesos de carga, descarga o actualización de aplicaciones, asi como servir de interfaz con otros sistemas que administran las transacciones electrónicas derivadas del uso de las tarjetas.

2.5.2.5 Quinta fase del ciclo de vida

La quinta fase 5 del ciclo de vida de las tarjetas inteligentes de acuerdo con la norma ISO 10202-1 define todas las medidas relativas a la denuncia del uso de la tarjeta.

En concreto, estas medidas consisten en la desactivación de las aplicaciones de la tarjeta inteligente, seguido por la desactivación de la tarjeta inteligente en sí.

Sin embargo, ambos procesos son teóricos en la mayoría de tarjetas inteligentes, excepto en los casos de reporte por robo o extravió.

Hay comandos que pueden utilizarse para desactivar las aplicaciones individuales y la tarjeta inteligente completa. En la norma ISO/IEC 7816-9 los comandos DELETE FILE, DEACTIVATE FILE, TERMINATE DF y TERMINATE CARD USAGE están expresamente destinados a ser utilizados para anunciar la etapa final del ciclo de vida de un aplicación.

Estos comandos son principalmente esenciales para la gestión de las aplicaciones individuales en tarjetas multiplicativas, pero rara vez se usan con las actuales tarjetas inteligentes, que incorporan en su mayoría sólo una aplicación. La forma más fácil de poner fin a la vida de una tarjeta inteligente es simplemente cortar en pedazos con unas tijeras.

La funcionalidad del SGTI, para esta fase del ciclo de vida de las tarjetas consiste en mantener actualizados los movimientos que reflejan el cambio de estado y transiciones que ocurren en la tarjeta por las condiciones de operación o reporte de extravió o robo.

El flujo que ocurre durante las transiciones de estados del ciclo de vida de una tarjeta se muestra en la figura 10.

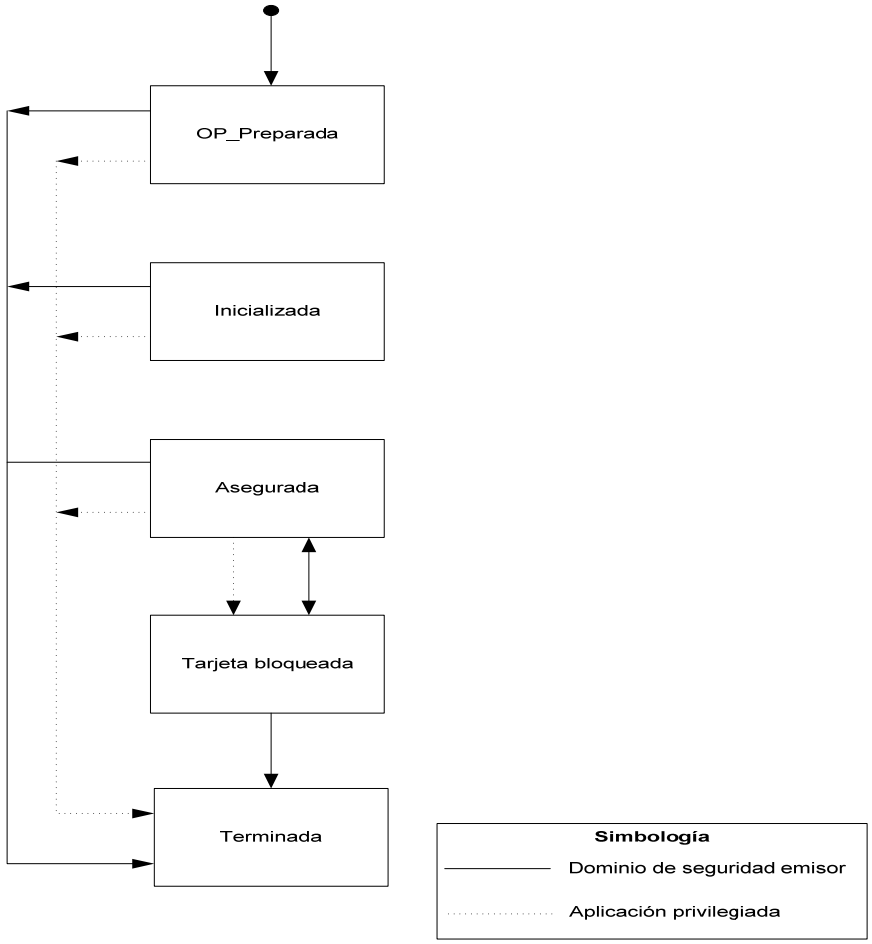


Figura 10. Diagrama de transición de los estados del ciclo de vida de la tarjeta

2.5.3 Ciclo de vida y estados de las aplicaciones

Los estados del ciclo de vida de las aplicaciones que están contenidas en las tarjetas inteligentes, establecen las condiciones para estar disponibles en cualquier momento, puedan ser bloqueadas de manera temporal o definitiva o puedan ser removidas de la localidad asignada.

De acuerdo a la especificación de Global Platform [W7] las aplicaciones pueden estar en cualquiera de los tres estados siguientes:

- Instalada
- Seleccionable
- Bloqueada

Donde la propia aplicación puede definir la dependencia entre los estados.

Instalada, señala que el código ejecutable de la aplicación está apropiadamente encadenado y que puede tomar lugar en cualquier alojamiento de memoria.

Seleccionable, la aplicación está disponible para recibir comandos por entidades desde fuera de la tarjeta. El estado de transición desde Instalada a Seleccionable es irreversible. La aplicación deberá estar instalada adecuadamente y estar funcional antes de que se asigne el estado Seleccionable.

La transición a Seleccionable puede ser combinada con el proceso de instalación de la aplicación.

Bloqueada, una entidad autenticada desde fuera de la tarjeta por un dominio de seguridad del emisor usa el estado bloqueado como un manejo de control de seguridad para prevenir la selección y la ejecución de la aplicación.

Las transiciones entre estos estados son las siguientes:

Bloqueada desde Instalada ←---------→ Instalada

Bloqueada desde Seleccionable ←--→ Seleccionable

Bloqueada desde un estado especificado <-> Estados específicos de la aplicación

por la aplicación

Timothy Juerguensen [21], presenta un modelo de ciclo de vida de las aplicaciones, considerando el punto de arranque a partir de que el desarrollo de la aplicación está concluido, quedando en condiciones de poder utilizarse, este estado se denomina Archivada, pasando posteriormente al estado de Cargada, estado cuya característica es que está alojada en una localidad válida de memoria pero aún no puede ser ejecutada.

El estado de Instalada establece las condiciones para la ejecución del código.

Cuando esta condición se da, se dice que entra al estado en Uso, que es propiamente cuando la aplicación se está ejecutando.

Desde el estado de en Uso, la aplicación puede cambiar a los estados Bloqueada o Borrada.

La transición entre Borrada y en Uso es reversible, mientras que la transición entre en Uso hacia Borrada es irreversible.

Los estados de transición están definidos en la tabla 8, y se muestran en la figura 11.

En la figura 12 se muestran las transiciones de los estados del ciclo de vida del dominio de seguridad.

La funcionalidad del SGTI, con relación al ciclo de vida de las aplicaciones consiste en mantener actualizado el perfil de las aplicaciones, los estados en que se encuentran a partir de la operación en campo de las tarjetas, eventos que ocurren principalmente en la etapa de postemisión, así como ser la interfaz con otros sistemas que gestionan las transacciones electrónicas que ocurren durante el uso de la tarjeta.

Tabla 8. Estados de transición de una aplicación

Estado anterior	**Estado nuevo**	**Criterio**
Archivada	Cargada	Escritura de código desde el servidor a EEPROM
Cargada	Instalada	Encadena la aplicación con el mecanismo de selección de la aplicación de la tarjeta
Instalada	En uso	Activación inicial para un arranque de la aplicación contexto
En uso	Bloqueada	Detección de uso no autorizado o uso inapropiado
Bloqueada	En uso	Recepción de aplicación válida con mensaje de desbloqueo
Bloqueada	Borrada	Borrado del EEPROM la aplicación manejada
En uso	Borrada	Remover del programa desde el mecanismo de selección de la aplicación

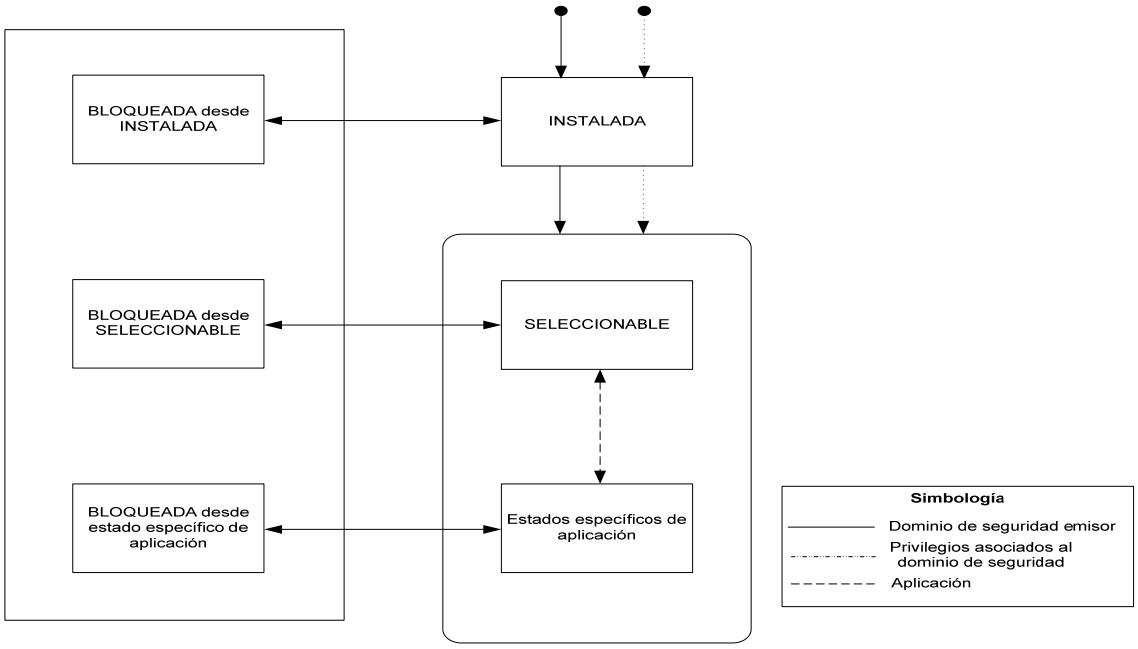


Figura 11. Diagrama de transición de los estados del ciclo de vida de las aplicaciones

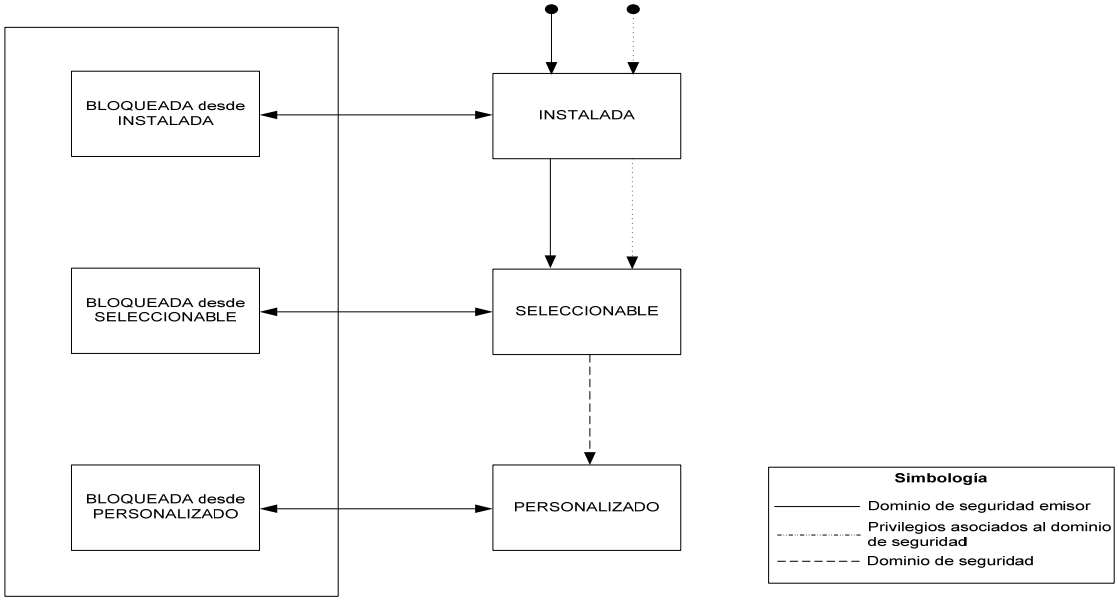


Figura 12. Diagrama de transición de los estados del ciclo de vida del dominio de seguridad

2.5.3.1 Aplicaciones y multiaplicaciones en tarjetas inteligentes

Hay una amplia gama de aplicaciones potenciales para las tarjetas inteligentes. El aspecto decisivo es que la aplicación general corre en la tarjeta inteligente como otra más de las aplicaciones dentro de la tarjeta y que la parte que se aplica en las terminales o los sistemas de nivel superior son las aplicaciones que están ubicadas fuera de la tarjeta.

Las diversas aplicaciones pueden clasificarse en aplicaciones cerradas y abiertas. En el caso de una aplicación cerrada, todo el sistema está bajo el control de una sola entidad, como cuando se utilizan tarjetas inteligentes, como tarjetas de identificación de una empresa. Por el contrario, las aplicaciones abiertas involucran a los participantes adicionales que se integran en el sistema, pero no pertenecen al operador del sistema. Probablemente el mejor representante de estos sistemas son las tarjetas de crédito.

En tal sistema, el emisor es un banco, el operador del sistema es una organización internacional que activa las tarjetas de crédito, y los comerciantes locales.

2.5.3.2 Tipos de aplicaciones

La mayoría de las aplicaciones de computadoras personales están basadas en archivos de código o sitios web, que muestran archivos en formato HTML con la ayuda de un navegador, son ejemplos típicos de aplicaciones basadas en archivos. El otro tipo de aplicación para computadoras personales se basa en la ejecución de un programa, como un programa de procesamiento de palabras. Estas aplicaciones además de la entrada del proceso y los datos de salida, requieren además un software ejecutable en el sistema destino.

Aplicaciones basadas en memoria

Las tarjetas de memoria, que no contienen medios de transformación de datos, se pueden utilizar para poner en práctica aplicaciones basadas en la memoria, que son técnicamente poco sofisticadas, pero sin embargo, adecuadas para el propósito de muchos casos. En tales aplicaciones, la terminal puede acceder a la totalidad de memoria para leer y escribir operaciones. Algunas tarjetas de memoria necesitan ciertas condiciones que deben cumplirse antes que dicho acceso sea posible, como un Pin de verificación o autenticación de la tarjeta de memoria. Sin embargo, la lógica de acceso necesaria para este propósito está en el cableado de los chips de memoria individual y no puede ser modificado. La figura 13 muestra la arquitectura de una aplicación basada en memoria de la tarjeta inteligente. Aplicaciones sencillas se pueden desarrollar utilizando este tipo de tarjeta, pero son limitadas en términos de su complejidad.

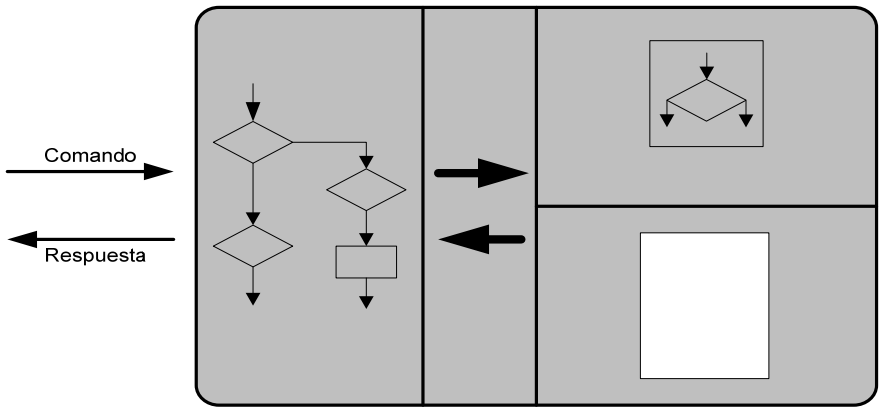


Figura 13. Arquitectura de una aplicación basada en la memoria de la tarjeta

Aplicaciones basadas en archivos

Las aplicaciones basadas en archivos requieren tarjetas con procesador y un sistema operativo que se ejecute en estas tarjetas. Puede estar implementada una aplicación en una tarjeta inteligente o varias aplicaciones en una tarjeta inteligente multiaplicación.

Una aplicación basada en archivos, normalmente adopta la forma de un conjunto de archivos de datos (EF), ubicado en un archivo de directorio (DF). Además, las condiciones de acceso para la lectura, la búsqueda, escritura, creación y supresión de los archivos de datos se especifican por un conjunto de reglas. El sistema operativo de las tarjetas inteligentes ofrece un gran número de comandos para el acceso a datos, la autenticación y otras operaciones. Alternativamente, las aplicaciones basadas en archivos pueden construirse utilizando objetos de datos (DOS). La figura 14 muestra la arquitectura de una aplicación basada en archivos de tarjeta inteligente.

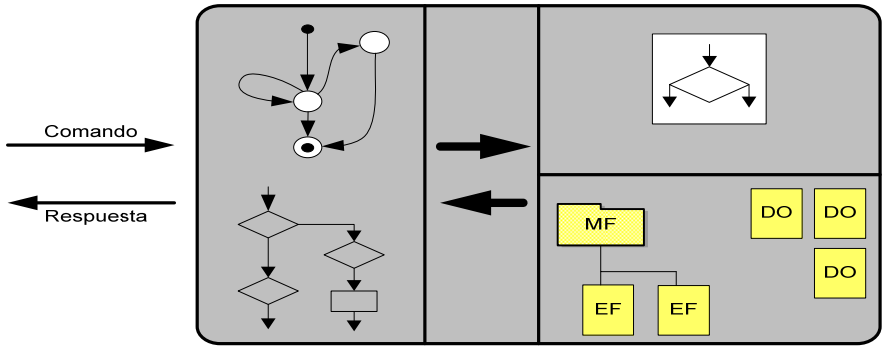


Figura 14. Arquitectura de una aplicación basada en archivos

Aplicaciones basadas en código

Las aplicaciones basadas en código, también utilizan archivos de datos, pero los archivos son complementados por código de programa que puede ser ejecutado en la tarjeta inteligente. Este código generalmente es una aplicación applet Java que se gestiona mediante mecanismos OPEN (ambiente general de Global Platform). La figura 15 muestra la arquitectura de una petición basado en código.

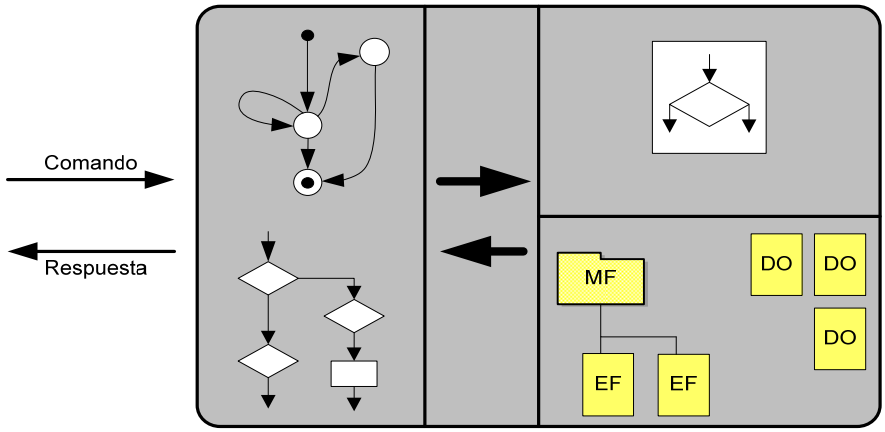


Figura 15. Arquitectura de aplicación basada en código

Las aplicaciones basadas en código dan a los desarrolladores de aplicaciones mayor grado de libertad, ya que los comandos adicionales permiten determinar y ampliar el alcance funcional de las tarjetas inteligentes. Sin embargo, esta libertad mayor es también una fuente de errores e incompatibilidades. Este tipo de aplicaciones sólo debe usarse si los requisitos no pueden cumplirse confiablemente a través de una aplicación basada en archivos, y es adecuada para su uso por los desarrolladores que tienen bastante experiencia en la programación de las tarjetas inteligentes.

2.5.4 Implementación del ciclo de vida de tarjetas y aplicaciones

De acuerdo a los estándares ISO/IEC 7816 [W15], ISO/IEC 14443 [W15], ISO/IEC 24727 [W15] y las especificaciones recomendadas por Global Platform [W7], a continuación se presentan los comandos APDU (Application Protocol Data Unit) para la transferencia y comunicación de datos, aplicables para la gestión de los estados del ciclo de vida, aclarando que para cada implementación en particular se debe de consultar el conjunto de instrucciones APDU del sistema operativo del ambiente de la tarjeta.

Del apartado de sistemas operativos, de este trabajo, se reproducen a continuación en la tabla 9.

Tabla 9. Comandos definidos por ISO/IEC 7816-4,-8-9 y Global Platform

Función	Comando	Descripción
Archivo	SELECT	Selecciona una operación de archivo
	READ BINARY READ RECORD	Lee datos desde un archivo transparente o reorientado
	UPDATE BINARY UPDATE RECORD	Escribe datos en un archivo transparente o reorientado
	SEARCH BINARY SEARCH RECORD	Búsqueda de acuerdo a un patrón en un archivo transparente o reorientado
Gestión de archivos	CREATE FILE	Crea un archivo (DF o EF)
	APPEND RECORD	Crea un registro nuevo en un archivo orientado por registros
	ACTIVATE FILE	Desbloquea reversiblemente un archivo
	DEACTIVATE FILE	Bloquea reversiblemente un archivo
	TERMINATE DF/EF	Bloque permanentemente un archivo (DF o EF)
	DELETE FILE	Borra un archivo (DF o EF)
Datos objetos	GET DATA	Lee datos objetos TLV
	PUT DATA	Escribe datos objetos TLV
Seguridad	VERIFY	Verifica la transferencia de datos
	GET CHALLENGE	Requiere un número aleatorio (ejemplo: para una posterior externa)
	INTERNAL AUTHENTICATE	Autenticación unilateral de una tarjeta por el mundo externo
	EXTERNAL AUTHENTICATE	Autenticación unilateral del mundo exterior por una tarjeta
	MUTUAL	Autenticación mutua de la

Función	Comando	Descripción
	AUTHENTICATION	tarjeta y el mundo exterior
	PERFORM SECURITY OPERATION	Ejecuta un algoritmo criptográfico en la tarjeta
	MANAGE SECURITY ENVIRONMENT	Maneja parámetros de comandos de seguridad
Administración de código de programas	LOAD	Carga una aplicación basada en código
	INSTALL	Instala una aplicación basada en código
	PUT KEY	Carga una llave para una aplicación basada en código
	SET STATUS	Escribe información del estado del ciclo de vida de la tarjeta o de una aplicación
	GET STATUS	Lee el estado de la información acerca del dominio de seguridad, carga de archivos o aplicaciones
	DELETE	Borra un objeto
Transmisión de datos	GET RESPONSE	Requiere datos para protocolos de transmisión T=0 desde la tarjeta

En el Anexo 1 se muestra en una tabla la relación de los comandos APDU y los estados del ciclo de vida.

Finalmente, podemos decir que en este apartado hemos revisado los conceptos del ciclo de vida de las tarjetas y de las aplicaciones que se cargan en ellas, los cuales son los procesos más importantes que gestiona el SGTI desde fuera de la tarjeta. Así también se ha referido a la interfaz existente entre la tarjeta y el SGTI, la cual está gobernada por los comandos APDU del sistema operativo de la tarjeta inteligente.

2.6 Criptografía y algoritmos

Una de las fortalezas del empleo de las tarjetas inteligentes, es la capacidad de poder registrar, almacenar y recuperar información con altos niveles de seguridad, requisito que otros tipos de tarjeta no pueden lograr.

Los componentes de hardware y software con que cuentan las tarjetas inteligentes a través de los microprocesadores proporcionan la capacidad y potencialidad de

utilizar mensajes cifrados, es decir información transformada que oculta su verdadero significado.

Como lo establece Daltabuit [1], la criptografía, es el arte de enmascarar los mensajes con signos convencionales, que solamente cobran sentido a la luz de una clave secreta.

Continuando con Daltabuit [1], los procesos de cifrado y descifrado son las operaciones fundamentales en la criptografía, la cual es entendida como un conjunto de técnicas que operan sobre los mensajes para convertirlos en representaciones que carecen de sentido para quien no deba recibirlo. Estas operaciones integran lo que se conoce como algoritmo criptográfico o algoritmo de cifrado E y que, junto con el elemento único de la transformación conocido como clave, el mensaje M a cifrar o mensaje en claro y el mensaje cifrado C conforman, todos, los elementos del sistema de cifrado o criptosistema.

La criptografía simétrica usa una misma clave secreta K para el proceso de cifrado y descifrado. Esta clave secreta es convenida entre el emisor y receptor del mensaje, estando la fortaleza del proceso en el nivel de secrecía en que se mantenga.

La criptografía asimétrica o de llave pública está soportada en una clase de funciones unidireccionales con trampa. En los cifrados asimétricos o de llave pública la clave de descifrado no se puede calcular a partir del cifrado.

La criptografía asimétrica tiene su fundamento en encontrar un sistema de cifrado computacionalmente viable y no complicado, de tal manera que el proceso de descifrado computacionalmente sea inviable a menos que se conozca la clave.

Para estos sistemas se usa una clave de cifrado (clave pública) K que determina la función trampa T y una clave de descifrado (clave privada) que permite el cálculo de la inversa de T.

Esto da la ventaja de que cualquier usuario puede utilizar la clave de cifrado, pero únicamente los usuarios indicados pueden conocer la clave privada para descifrar correctamente.

Este enfoque respeta el manejo público, tal como sucede con el cifrado simétrico, donde los procesos de cifrado y descifrado son públicos, residiendo la fortaleza del proceso en la llave privada.
Tal como lo refiere Daltabuilt [1], la construcción de un criptosistema de clave pública está dado por la siguiente secuencia de recomendaciones:

- Escoger un problema difícil P, de ser posible intratable
- Escoger un sub problema de P fácil, que se resuelva en tiempo polinomial preferiblemente en tiempo lineal [W1]

- Transformar el problema P fácil de tal manera que el problema resultante P difícil, no se parezca al inicial, pero si al problema original P
- Publicar el problema P difícil y la forma en que debe de ser usado, constituyendo este proceso en la clave pública de cifrado
- La información sobre cómo se puede recuperar el problema P fácil a partir del problema P difícil se mantiene en secreto y constituye la clave privada de descifrado.

Los sistemas criptográficos que están embebidos en los microprocesadores de las tarjetas inteligentes en la actualidad tienen disponibles los sistemas criptográficos simétricos AES, DES, 3DES, mientras que para sistemas criptográficos asimétricos están disponibles RSA y Curvas Elípticas.

2.6.1 Algoritmo DES

La descripción del algoritmo Data Encryption Standard (DES), publicado por el NIST (National Institute of Standards and Technology) [W3] y [W19] especifica dos algoritmos criptográficos FIPS aprobados, requeridos por FIPS (Federal Information Processing Standards) 140-1, cuando se utiliza con el estándar estadounidense X9.52(ANSI, American National Standards Institute) [W41]. Esta publicación ofrece una descripción completa de los algoritmos matemáticos para el cifrado y descifrado de información codificada binaria. Fue publicado en 1977 como FIPS PUB46 y posteriormente en 1981 fue aprobado como estándar por la ANSI.

De acuerdo con Maiorano [38], DES es un algoritmo cifrado por bloques, que cifra información en bloques de 64 bits de longitud. En el cifrado, un bloque de este tamaño será entrada del algoritmo, el texto plano y, junto con la llave se producirá una salida de la misma longitud que es el texto cifrado.

El algoritmo utiliza una substitución seguida de una permutación del texto de entrada, en función de la llave. Esta operación se conoce como ronda. DES realiza 16 rondas.

2.6.2 Algoritmo 3 DES

La definición del algoritmo 3DES publicada por el NIST [W4] refiere que 3DES, no llega a ser un cifrado múltiple, porque no son independientes todas las subclases.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con dos claves diferentes se aumenta el tamaño efectivo de la clave.

Triple DES, TDES, es un algoritmo formado a partir del algoritmo DES. Básicamente se realiza el proceso DES tres veces y es también del tipo de cifrado por bloques.

El algoritmo opera en bloques de 64 bits de longitud del texto de entrada. Luego de una permutación inicial, el bloque es dividido en dos bloques de 32 bits. Se aplican las 16 rondas, de las mismas operaciones, en las cuales la información es combinada con la llave. Luego de las 16 rondas, las dos mitades citadas, vuelven a juntarse para dar lugar a la última permutación.

Si Bi es el resultado de la iteración número i, Li y Ri son las dos mitades de Bi, Ki la llave para la ronda i y f la función que aplica sobre la llave (permutaciones, transposiciones, operaciones XOR), una ronda implicará que:

Li = Ri-1
Ri = Li-1 XOR f (Ri-1, Ki)

2.6.3 Algoritmo AES

De acuerdo a la publicación del NIST [W2], el algoritmo AES (Advanced Encryption Standard) es una norma que especifica el algoritmo Rijndael [W2]. El cual es un sistema de cifrado simétrico de bloques con el que se pueden procesar bloques de datos de 128 bits, utilizando claves de cifrado con longitudes de 128, 192, y 256 bits.

Rijndael fue diseñado para manejar tamaños de bloques y longitudes de clave adicionales [R8]. Fue anunciado por el NIST en el año 2001 como estándar y a partir de 2002 como un estándar FIPS PUB 197.

AES permite un mayor rango de tamaños posibles de bloques y de longitudes de llaves. AES especifica un tamaño de bloque fijo de 128 bits de longitud; para la lleve tamaños de 128, 192 o 256 bits.

AES utiliza lo que se conoce como campo Galois (dominio de redefinición de operaciones matemáticas)

2.6.4 Algoritmo RSA

Siguiendo a Death Master [R23] y de acuerdo con los sitios [W35], [W36] y [W37], RSA es el algoritmo asimétrico de cifrado más usado, Las longitudes de clave usadas hoy en día varían desde los 512 hasta los 4096 bits, aunque se suelen tomar de forma habitual claves de 1024 bits puesto que las de 512 bits no se consideran suficientemente seguras. Este tamaño puede parecer pequeño, pero permite la generación de claves de longitudes de hasta 1233 cifras con 4096 bits

Para este apartado, podemos concluir que los algoritmos criptográficos revisados, se ejecutan en el hardware y software del microprocesador embebido en la tarjeta, con el propósito de realizar la protección de los datos durante la ejecución de las aplicaciones y la comunicación de la tarjeta con el exterior, representado por el

SGTI y la infraestructura de terminales dispuesta para la operación del programa de tarjetas.

2.7 Arquitectura de la tarjeta

En este apartado estudiamos la arquitectura de la tarjeta inteligente, asociado con las funcionalidades del sistema operativo, los mecanismos del ambiente de las multiaplicaciones, el intercambio de datos internos/externos, los dominios de la seguridad y la administración del ciclo de vida.

Como referencia de la arquitectura de la tarjeta se toma Global Platform e ISO 7816-13 [R7] y como ambiente de ejecución Java Card [R22].

2.7.1 Java Card

De acuerdo a las especificaciones publicadas por Sun Microsystems [W8] y al análisis realizado por Mike Hendry [19], Java es un lenguaje interpretado diseñado para cumplir con el criterio de "escribir una vez, utilizar en cualquier lugar".

Java Card realiza la misma función, pero dentro del limitado medio ambiente de la tarjeta inteligente: los programas Java creados para un entorno generalmente de navegador no se ejecutan en una tarjeta inteligente, porque la tarjeta cuenta con recursos mucho más limitados.

Tampoco los applets Java Card son compatibles con el ambiente Java, sino que son diseñados para cumplir con la norma ISO/IEC 7816 referente a nombres de archivos, selección de aplicaciones y estructuras de archivos, así como el tener en cuenta las características operativas y técnicas de la tarjeta inteligente: como por ejemplo, el distinguir entre la RAM y EEPROM como medio de almacenamiento de datos.

Java Card define:

- Un subconjunto del lenguaje Java, que elimina las funciones inteligentes no pertinentes para la tarjetas y otros pequeños sistemas incorporados
- Una estructura para la definición de los requisitos, de tiempo de ejecución del programa, para la elaboración, las pruebas y generar el bytecode compilado o preprocesado del programa en Java
- Un entorno de ejecución que permite que el bytecode de Java se ejecute en el hardware de los diferentes fabricantes

El último de estos, es la responsabilidad de cada fabricante de tarjetas inteligentes el ofrecer una interfaz de Java Card, ya que depende de las características particulares que ofrece el hardware, de los componentes de la tarjeta y del sistema operativo, véase la figura 16.

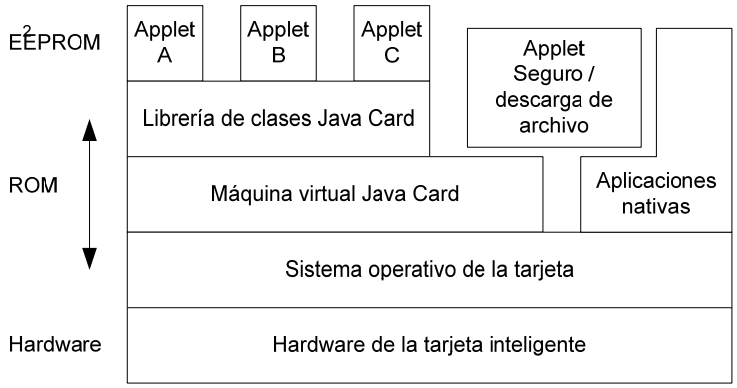


Figura 16. Entorno de ejecución de Java Card

Una aplicación de Java Card consta de un applet (el código de bytes almacenados en la tarjeta), que llama a un conjunto de bibliotecas de clases, como lo explica Chen [12].

No se puede cargar y utilizar en tiempo real, pero se le da el nombre porque puede ser descargado en la tarjeta después de que la tarjeta fue expedida, y es probable que se almacene en la memoria dinámica (normalmente en el EEPROM.

El sistema de bibliotecas de clase normalmente se almacenan en la memoria ROM, otras clases definidas por el usuario por lo general se cargan en EEPROM. El sistema de librerías de clases Java Card cubren la gama de funciones que necesitan los programas de Java Card, y que representan un rango mucho menor que los applets de Java, a causa del rango menor de las clases y los métodos permitidos por Java Card. Por ejemplo, Java Card no utiliza los tipos de datos de punto flotante, cadenas o matrices de varias dimensiones, el encadenado no es soportado.

Esta estructura ofrece dos de los principales beneficios de Java Card: portabilidad y la familiaridad. En principio (y cada vez más en la práctica), las aplicaciones Java Card son portables a través de las implementaciones de Java Card de diferentes fabricantes. Muchos programadores están familiarizados con las estructuras de Java, haciendo más fácil su rol en la programación de tarjetas inteligentes

El lenguaje Java hace uso de una máquina virtual, una máquina virtual de Java (JVM por sus siglas en inglés) tiene todo el conocimiento y los recursos que necesita para ejecutar el bytecode de Java en un entorno de hardware en particular. La máquina virtual Java Card (JCVM por sus siglas en inglés) difiere de la mayoría de las JVM, se divide en dos: la tarjeta inteligente solamente contiene las funciones pertinentes al tiempo de ejecución, mientras que otras funciones como la clase de carga, de vinculación y control de código de bytes se llevan a

cabo por un programa convertidor, que se ejecuta en una plataforma PC o estación de trabajo.

Esta estructura permite a la JCVM ser tan pequeña como sea posible, un requisito clave para un entorno de tarjetas inteligentes. Los kits de herramientas de desarrollo, por lo general también contienen un emulador de JCVM, que permite al programador probar la mayoría de las funciones de la aplicación (pero no, en la mayoría de los casos, la interacción entre aplicaciones) en la plataforma de PC antes de cargar en la tarjeta. También contiene el paquete de instalación necesario para cargar los applets a la tarjeta. La figura 17 muestra un entorno típico de desarrollo de Java Card.

El entorno de ejecución Java Card (JCRE por sus siglas en inglés) es la parte de la estructura de Java Card que debe ser proporcionada por el proveedor de tarjetas inteligentes: el hardware, sistema operativo de tarjetas, componentes de tiempo de ejecución de la JCVM y las librerías de clases.

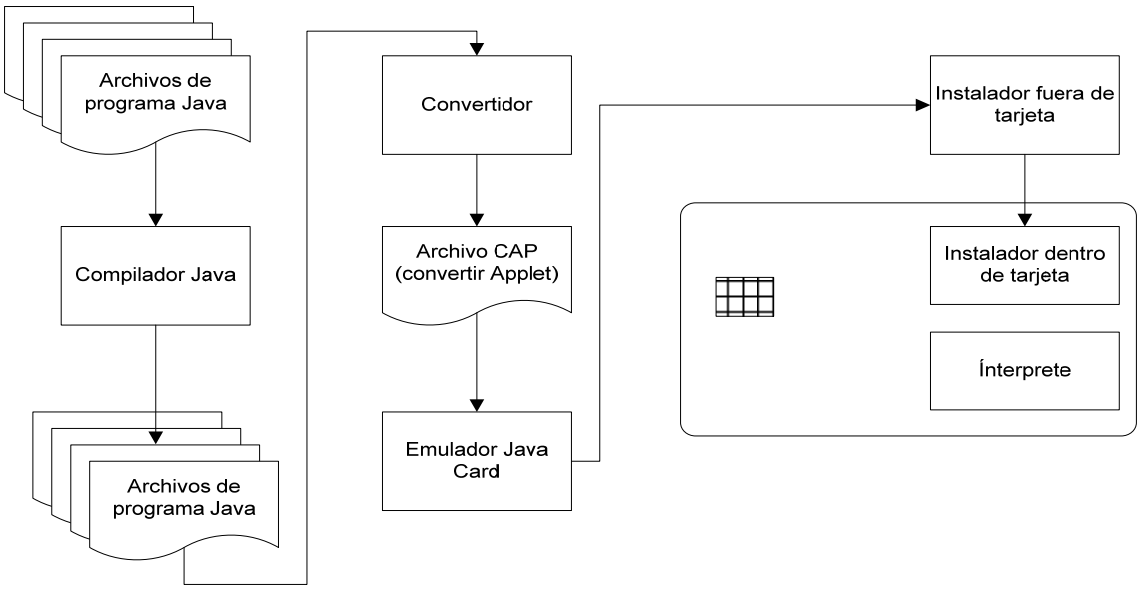


Figura 17. Ambiente de desarrollo de Java Card

La JCRE también por lo general contiene la mitad del programa de instalación, Java Card por sí mismo no define completamente este proceso, y aquí es donde Global Platform fortalece estos procesos. Se puede tener un JCRE que no contiene un instalador, en este caso las peticiones se deben cargar durante la inicialización de la tarjeta o proceso de personalización. Estas tarjetas se conocen como Java Card-S, o Java Card estática; que son generalmente más baratas que

otras Java Card y pueden ser una buena opción en los entornos operativos donde descargar postemisión no es un problema.

Una característica importante de la JCRE, es que corre todo el tiempo que se mantenga conectada la tarjeta. Cada vez que la tarjeta se enciende, se reinicia el JCRE y recupera desde la memoria su estado anterior, que permite a la tarjeta recuperarse de cualquier error en los datos.

Un aspecto destacado de Java Card es su modelo de seguridad, el emisor de la tarjeta le otorga un alto grado de flexibilidad en cuanto al nivel del control que ejerce sobre los applets y objetos de datos sobre la tarjeta. Los applets convertidos (conocido como PAC de archivo) se firman en un paquete por el emisor mediante una clave secreta DES y los controles de esta firma (usando la misma clave) cuando se carga el archivo de la PAC.

Para la comprobación de tiempo de ejecución, en lugar de la caja de arena que normalmente se asocia con Java, Java Card utiliza un mecanismo de firewall por software que vincula explícitamente cada objeto con el applet que posee, e impide el acceso a los objetos por otros applets. Estos dos mecanismos en conjunto permiten al emisor de la tarjeta diseñar las estructuras de seguridad para las tarjetas multiaplicación, con uno o más emisores de aplicación, los canales de carga, y con niveles de seguridad adecuados para la aplicación.

Estas características se definen con más detalle en las especificaciones Global Platform; aunque una Java Card estática (Java Card-S) puede ejecutar especificaciones sin Global Platform, una funcionalidad mucho más amplia se obtiene mediante la aplicación de Java Card y Global Platform juntos.

2.7.2 Global Platform

Global Platform [W7] es un consorcio que reúne a fabricantes de tarjetas inteligentes, empresas de software y sectores de usuarios (principalmente emisores, de las áreas de finanzas y telecomunicaciones). Tiene amplias competencias, por lo que se describe a sí misma como "la norma para la infraestructura de las tarjetas inteligentes" con la misión de "establecer, mantener e impulsar la adopción de normas que permitan un proceso abierto e infraestructura interoperable para tarjetas inteligentes, dispositivos y sistemas que simplifican y aceleran el desarrollo, despliegue y gestión de aplicaciones en las industrias.

2.7.2.1 Arquitectura Global Platform

Global Platform complementa y soporta el ambiente de Java Card, especificando los procesos para la carga y la gestión de aplicaciones de la tarjeta, así como también ofrece una arquitectura estándar de terminal que otorga beneficios similares para las terminales multiaplicación, y una norma como un conjunto de

comandos de personalización de tarjetas (carga de aplicaciones y parámetros antes de que la tarjeta sea emitida).

Tanto la tarjeta y la terminal pueden tener múltiples aplicaciones, pero no siempre tienen que ser de las mismas agrupaciones: véase las figuras 18 y 19.

La clave de la arquitectura de los sistemas que operan las tarjetas inteligentes es el reconocimiento de los roles que desempeñan las diferentes entidades empresariales en un entorno multiaplicación.

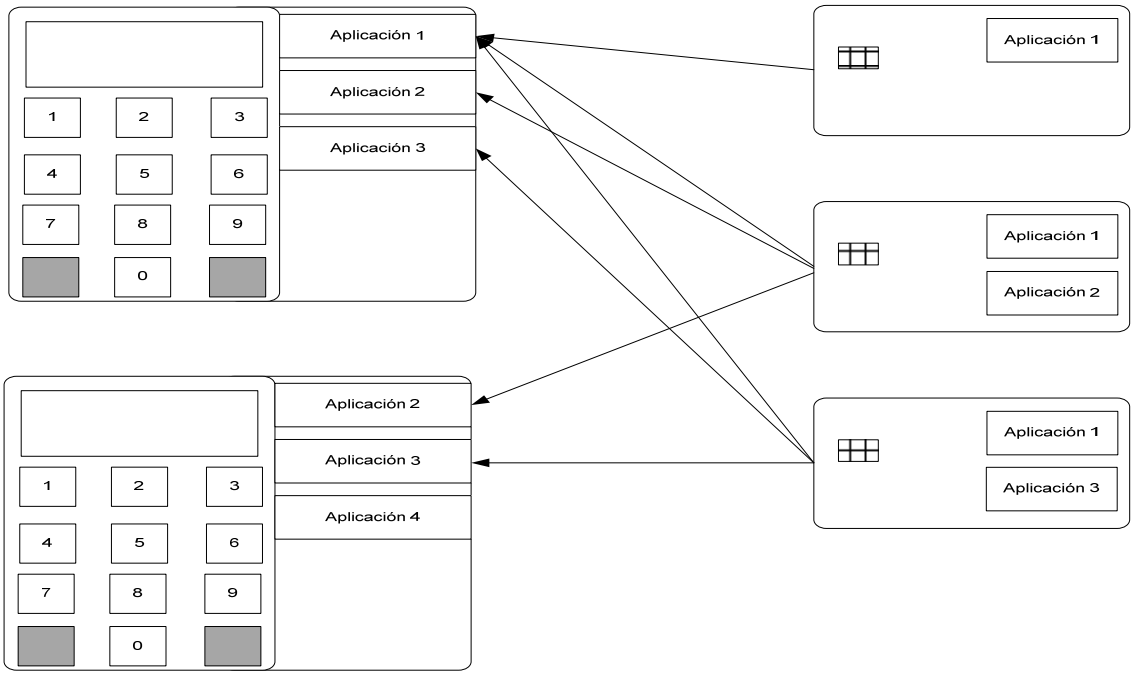


Figura 18. Tarjetas con múltiples aplicaciones y diferentes terminales

Considerando que para una aplicación única, la tarjeta puede, en principio, aceptar que el emisor de la tarjeta asuma la responsabilidad de todos los aspectos del desarrollo de la tarjeta, en la producción y uso, en una tarjeta multi aplicaciones, hay un conjunto complejo de relaciones entre los desarrolladores, implementadores y los usuarios operativos de la tarjeta. De hecho, incluso para un solo usuario de tarjeta, existen importantes ventajas técnicas, por ejemplo, asegurar que las llaves del emisor, se utilicen dentro del dominio del emisor y, por contrato, es importante ser capaz de definir las responsabilidades de un acuerdo de nivel de servicio.

Como lo establece el estándar ISO/IEC 7816-13 [W15], el Administrador de la tarjeta (Card Manager), describe la administración para una tarjeta multi

aplicaciones. Las llaves especiales y las aplicaciones de administración de la seguridad son llamadas Dominios de seguridad (Security Domains) los cuales son creados para asegurar una completa separación de las llaves del emisor y las de los múltiples proveedores de aplicaciones.

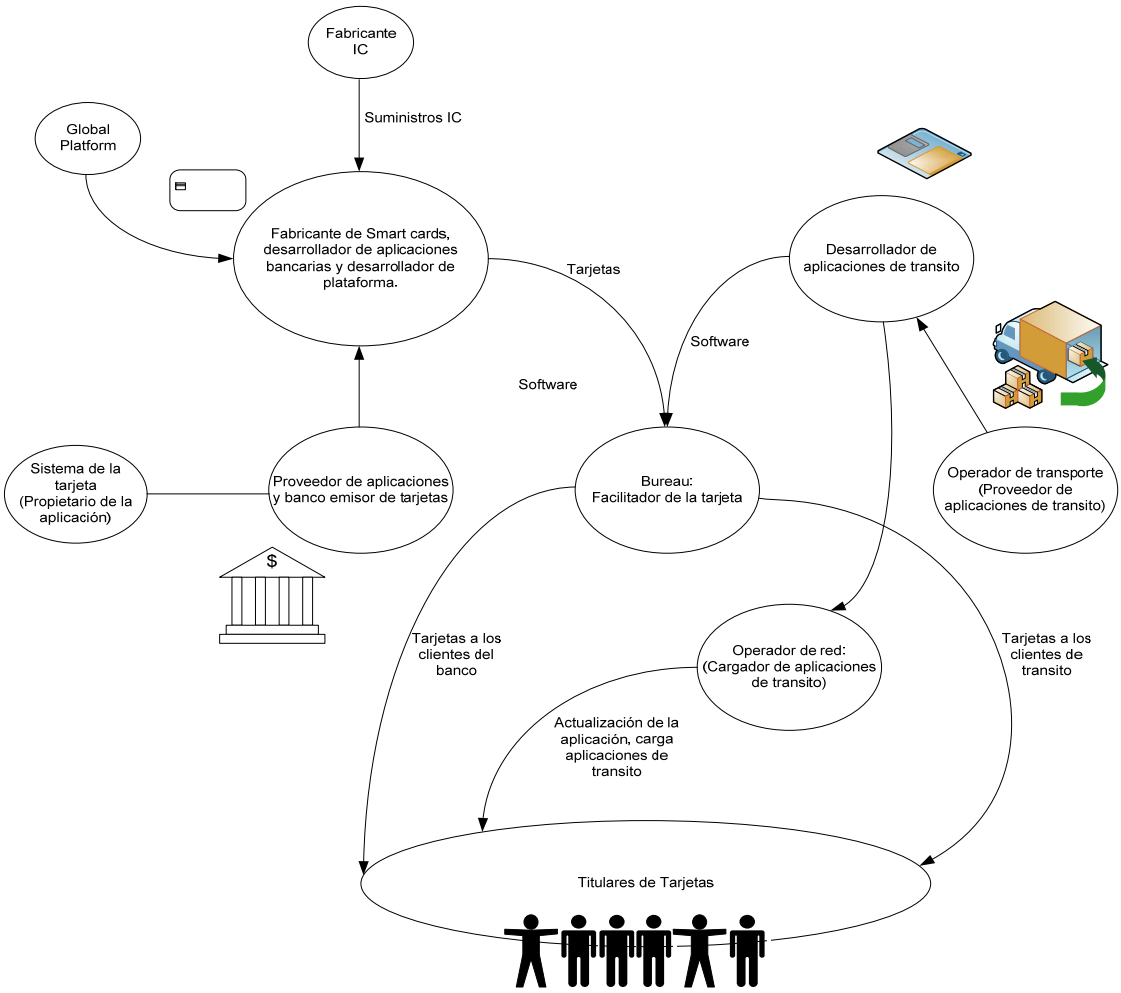


Figura 19. Interacción de aplicaciones entre las diferentes entidades empresariales

El Administrador de la tarjeta realiza las principales funciones para el acceso a las funciones sensibles de la misma, tales como la carga de una nueva aplicación actualizada, comprueba que las aplicaciones utilizan la memoria asignadas a ellas, comprueba cada comando APDU que llega a la tarjeta y envía a la aplicación seleccionada.

De acuerdo, a como lo señala Global Platform [W7] el Administrador de la tarjeta realiza un seguimiento del ciclo de vida de la tarjeta y de las aplicaciones, tal

como se describe a continuación, y gestiona la seguridad de la estructura del dominio. También proporciona un Pin global que se puede compartir entre las aplicaciones.

La aplicación Administrador de la tarjeta se complementa con una API en la tarjeta que se incrusta en la JCVM, también se puede incrustar en otros sistemas operativos de tarjetas, tal como Multos, lo que permite utilizar los sistemas operativos de las tarjetas para tomar ventaja de la tarjeta Global Platform y la aplicación de la gestión de las estructuras, véase la figura 20.

Esta API proporciona un número pequeño de funciones adicionales que se necesitan para aplicaciones de Global Platform por el Administrador de la tarjeta.

Utilizando estas funciones en una aplicación se puede, por ejemplo:

- Bloquear toda la tarjeta, si se considera que la seguridad de la tarjeta puede ser violada
- Abrir un canal seguro de comunicación externa de la tarjeta
- Comprobar un valor de llaves antes de cargar la llave de la tarjeta

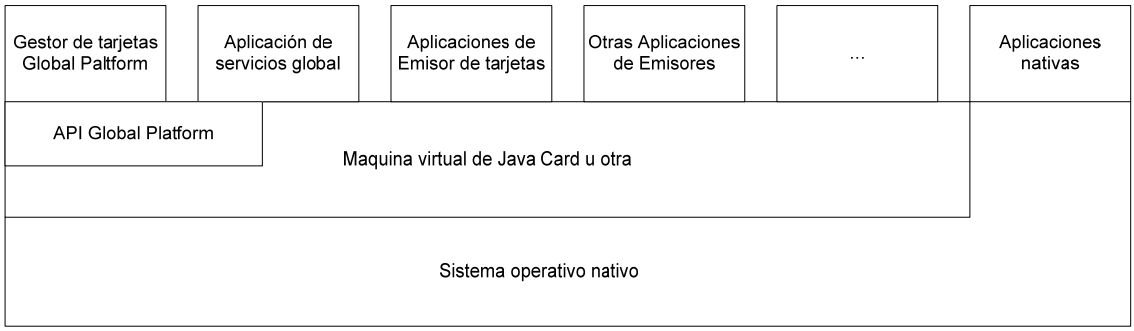


Figura 20. Ambiente Global Platform de multiaplicaciones/multiproveedores

El Administrador de la tarjeta controla el dominio de seguridad del emisor de la misma, maneja las llaves del emisor, establece un canal seguro para el emisor en caso necesario y controla los permisos para actividades tales como la carga de aplicaciones.

Global Platform también permite que el emisor cree dominios adicionales de seguridad en la tarjeta. Esto es probable que se necesite en una o más aplicaciones de la tarjeta que son controladas por organizaciones completamente diferentes.

Cada aplicación pertenece a un dominio de seguridad, como se observa en la figura 21, que representa los dominios para el régimen descrito en la figura 19.

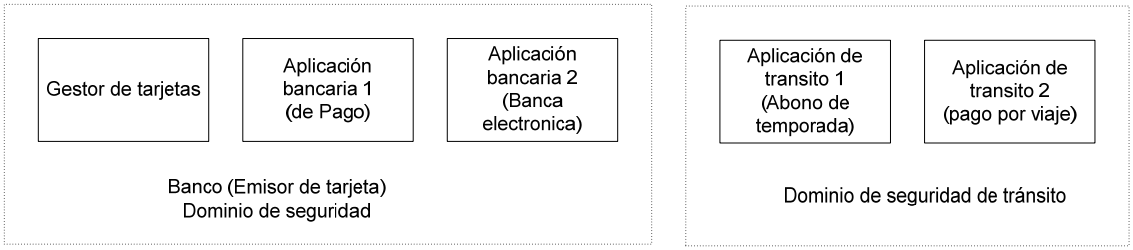


Figura 21. Dominios de seguridad de la arquitectura multiaplicaciones

Otro aspecto de la tarjeta y la gestión de aplicaciones dirigida por Global Platform es el ciclo de vida de la tarjeta y las aplicaciones. Se reconoce que las tarjetas pasan por una secuencia de estados tal y como se estudio en el capítulo anterior, y se muestra en la figura 22.

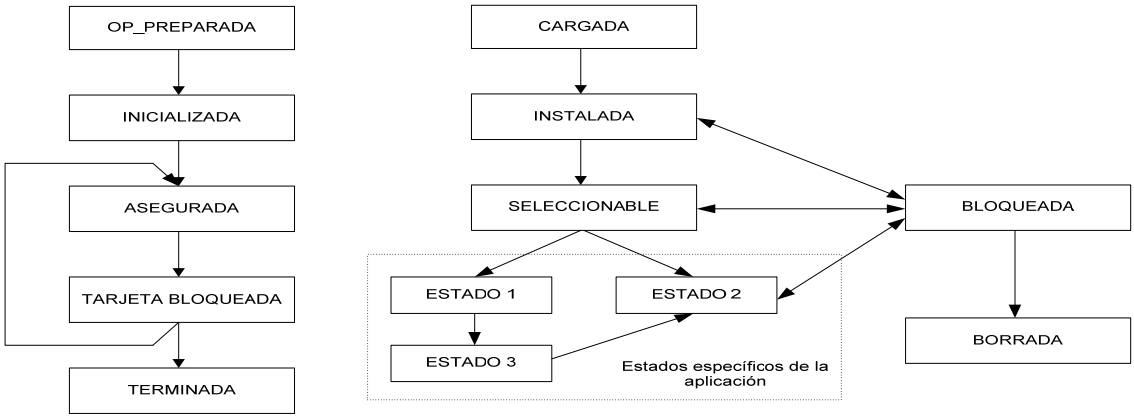


Figura 22. Ciclo de vida de la tarjeta y aplicaciones

El ciclo de vida de la tarjeta se inicia cuando la API de Global Platform y el Administrador de la tarjeta son cargados, lo siguiente es inicializar, para tener otras aplicaciones y parámetros en la misma carga, y se asegure antes de su emisión. Si se detecta un evento que afecte la seguridad, la tarjeta puede ser bloqueada, pero también puede ser desbloqueada (regresando al estado SECURED) por el emisor de la tarjeta. Si la tarjeta está terminada, entonces ya no puede ser restaurada o usada. La aplicación de estas reglas está en concordancia con los establecido y estudiado anteriormente en la parte 1 de ISO/IEC 10202.

El ciclo de vida de una aplicación es más específico y es gestionado por la propia aplicación utilizando las funciones de la API Global Platform. Una vez que la

aplicación se carga en la tarjeta, debe ser convertida en el formato de tiempo de ejecución (instalado) y entonces ya se puede seleccionar. En ese punto, puede ser seleccionada por una aplicación de terminal, hasta que sea bloqueada por la propia aplicación o por su propietario.

Una vez más, la correcta gestión de la tarjeta y los ciclos de vida de la aplicación son muy importantes en un ambiente multiaplicación, criterios de bloqueo de una tarjeta pueden ser muy diferentes de compañía a compañía.

La especificación de Dispositivos Global Platform (GPD por sus siglas en inglés) está basada en la Plataforma de Interoperabilidad de Pequeñas Terminales (STIP por sus siglas en ingles), los objetivos de esta especificación son:

- Permitir la portabilidad de código entre los diferentes tipos de terminales, como sucede con la especificación Java Card, una aplicación desarrollada para un terminal GPD debe correr sin modificaciones en otra terminal GPD
- Permitir que las aplicaciones de tarjetas y terminales que se desarrollaron se prueben juntas
- Reducir el costo y tiempo necesarios para desarrollar aplicaciones de terminal

Un dispositivo STIP contiene:

- Su propio sistema operativo: Puede ser un sistema operativo propietario, que incluya una gama de funciones adicionales y controladores de dispositivos para periféricos
- El entorno de ejecución de STIP: Es la interfaz entre el sistema operativo y el marco de referencia de operación básico STIP
- El marco de referencia de operación básico STIP API: Sea compatible con las solicitudes de acceso a los servicios del sistema operativo y los controladores de una manera coherente (se accede a todos los dispositivos utilizando los mismos métodos y llamadas)

También se incluye una API estándar para la activación de aplicaciones (conocidas como stiplets en el mundo STIP).

La especificación de dispositivos también incluye una especificación para la estructura interna del stiplet, dividiéndolo en el componente base de lógica, el cual es independiente de la plataforma o del ambiente en el que se ejecuta, y los servicios y funciones que dependen de la plataforma de la aplicación. Una vez más, la idea es reducir al mínimo la cantidad de trabajo necesario cuando una aplicación se transfiere de un tipo de terminal a otra.

La arquitectura de la tarjeta Global Platform se integra de una serie de componentes que garantizan que las interfaces del hardware de vendedores

neutrales, para aplicaciones dentro y fuera de los sistemas de gestión de la tarjeta funcionen sin problemas.

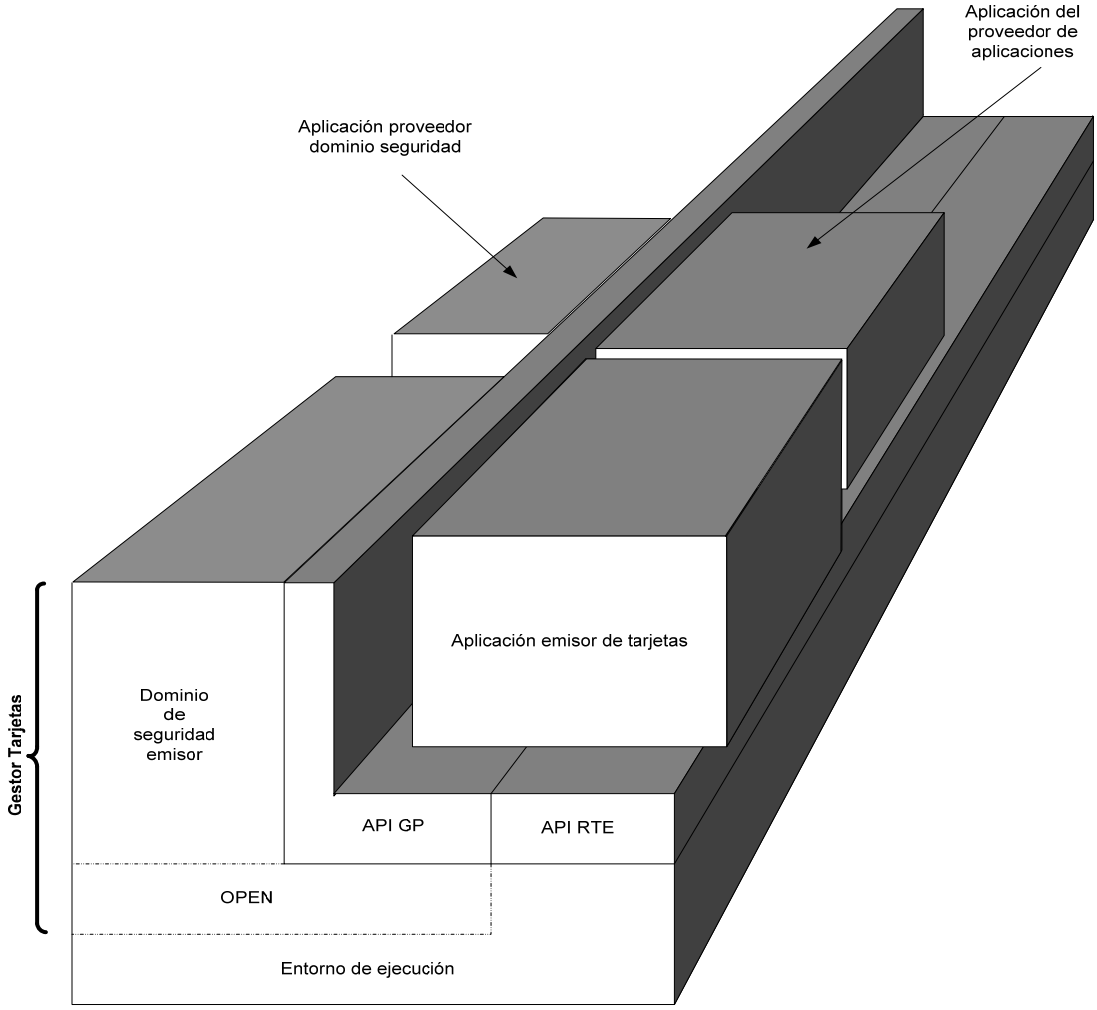


Figura 23. Arquitectura de la tarjeta Global Platform

De acuerdo a Global Platform [W7] y el estándar ISO/IEC 7816-13 [W15], la figura 23 muestra los componentes de una configuración de tarjeta que incluye una aplicación del Emisor de la tarjeta (Card Issuer) y una aplicación de los socios comerciales del emisor de la tarjeta referido como un Proveedor de aplicaciones (Application provider).

Todas las aplicaciones a ser implementadas en un ambiente de ejecución seguro incluyen un hardware neutral API (por sus siglas en inglés Application Programming Interface) para soportar la portabilidad de la aplicación.
Global Platform no obliga a una tecnología específica como ambiente de ejecución.

Global Platform se ejecuta en la parte superior de cualquier ambiente de ejecución seguro multiaplicativo. Este entorno de ejecución es el responsable de proporcionar una API hardware-neutral para aplicaciones, así como un espacio seguro de almacenamiento y ejecución de aplicaciones, para garantizar que el código de cada aplicación y los datos se mantengan separados y seguros de otras aplicaciones en la tarjeta.

Otra responsabilidad importante del Administrador de la tarjeta es ser el representante del emisor de la tarjeta.

El Administrador de la tarjeta puede ser visto como tres entidades:

- El Ambiente de Global Platform,
- El dominio de seguridad del emisor y,
- Los métodos de verificación del dueño de la tarjeta

Estas tres entidades están incorporadas como una o cada una puede ser vista como una entidad separada y distinta.

Las principales responsabilidades del Ambiente Global Platform (OPEN) son proporcionar una API para las aplicaciones, comandos para despachar, selección de aplicaciones, (opcional) gestión de canales lógicos, y administración del contenido de la tarjeta. Estas funciones están disponibles si no son facilitadas por el entorno de ejecución, o si son provistas por el entorno de ejecución de una manera que no cumplan con esta especificación.

El OPEN ejecuta el código de las aplicaciones relacionadas con la gestión del contenido de la tarjeta (Card Content Management).

El OPEN también gestiona la instalación de las aplicaciones cargadas en la tarjeta. El OPEN es responsable de los principios de seguridad definidas en la carga e instalación del contenido. Estos principios incluyen la verificación del código de aplicación y la autorización para la carga y/o la instalación ha sido proporcionada por el emisor de la tarjeta. Otra función importante, es el despacho de los comandos APDU y la selección de aplicaciones.
Cuando se recibe un comando SELECT, el OPEN asigna las aplicaciones referenciadas en el comando SELECT para seleccionar las aplicaciones y subsecuentes comandos de aplicaciones y se enviaran las aplicaciones seleccionadas.

La disponibilidad de canales lógicos introduce una adicional dimensión a la arquitectura de la tarjeta como múltiples aplicaciones que pueden ser seleccionadas concurrentemente. El OPEN, se basara en el entorno de ejecución para controlar cuando una aplicación individual pueda ser seleccionada

concurrentemente con otra aplicación. Cuándo soporte los canales lógicos, el OPEN permitirá que las aplicaciones que no tienen asignado canal lógico como son multiseleccionables. El soporte de los canales lógicos es opcional.

El OPEN tiene y usa un Registro Global Platform (GPR por sus siglas en inglés) interno como un recurso de información para la administración del contenido de la tarjeta. El Registro Global Platform, contiene información para administración de la tarjeta, archivos cargados ejecutables, aplicaciones, dominio de seguridad y privilegios.

2.7.2.2 Dominio de seguridad del emisor

El dominio de seguridad del emisor, es el programa obligatorio representativo del emisor de la tarjeta, tiene la capacidad de cargar, instalar y eliminar aplicaciones que pertenecen tanto al emisor de la tarjeta o aplicaciones de otros proveedores.

En muchos otros aspectos el dominio de seguridad del emisor, es muy similar a cualquier otro dominio de seguridad.

2.7.2.3 Dominios de seguridad

Así como el dominio de seguridad del emisor es el representante en la tarjeta del emisor de la tarjeta, el Dominio de seguridad del proveedor de aplicaciones (Application Provider Security Domain), se refiere como un dominio de seguridad, esta especificación es la del representante en la tarjeta de un proveedor de aplicación o de la autoridad del control.

Una autoridad de control puede existir, cuya función es hacer cumplir la política de seguridad en todo el código de la aplicación cargada a la tarjeta. Si es así, la Autoridad de Control también utiliza un dominio como su representante en la tarjeta.
Los dominios de seguridad soportan servicios de seguridad, tales como manejo de llaves, cifrado, descifrado, generación y verificación de firmas digitales de los propietarios (emisor de la tarjeta, proveedor de la aplicación o autoridad del control) de las aplicaciones.

El dominio de seguridad tiene características de aplicación, privilegios de la aplicación, y estados del ciclo de vida (el dominio de seguridad del emisor hereda el estado del ciclo de vida de la tarjeta). Un ejemplo del dominio de seguridad que funciona como una aplicación es cuando el dominio de seguridad es seleccionado para cargar una nueva aplicación a la tarjeta.
Cada dominio de seguridad implementa un protocolo de canal seguro (Secure Channel Protocol) definiendo la seguridad aplicada durante la comunicación entre el emisor de la tarjeta, el proveedor de aplicaciones o la autoridad del control y el dominio de la seguridad de la tarjeta.

El dominio de seguridad también proporciona una interfaz para aplicaciones para acceso a los servicios del dominio de seguridad. Tiene bien definidos la interfaz externa APDU para garantizar que todas las implementaciones del dominio de seguridad se comporten consistentemente y puedan ser gestionadas de forma idéntica por el mismo sistema de gestión de la tarjeta, externo a la tarjeta.

Como la mayoría de estos servicios y los comandos APDU están relacionados con el Contenido de la tarjeta (Card Content), el dominio de seguridad está estrechamente interrelacionado con el OPEN.

Cada dominio de seguridad establece el nombre del emisor de la tarjeta, un proveedor de la aplicación o una autoridad de control, cuando estas entidades fuera de la tarjeta requieren el uso de llaves que están completamente aislados unos de otros.

La API de Global Platform proporciona servicios a las aplicaciones (por ejemplo, la verificación del titular, la personalización, o los servicios de seguridad). También ofrece servicios al Administrador del Contenido de la tarjeta (por ejemplo, bloqueo de la tarjeta o actualización del estado del ciclo de vida de las aplicaciones).

El Contenido de la tarjeta (Content Card), tal como se define en la especificación Global Platform, está disponible en la tarjeta en la forma de un archivo de carga ejecutable. Un archivo de carga ejecutable puede existir en:

- Memoria inmutable persistente (ROM) en cuyo caso se carga durante la fase de fabricación y no puede ser alterado (excepto ser deshabilitado), o
- Memoria mutable persistente (EEPROM) en cuyo caso se puede cargar o remover durante la preemisión o postemisión.

Cada archivo de carga ejecutable puede contener uno o varios módulos ejecutables, empezando con código de aplicaciones. La instalación de una aplicación crea una instancia desde un módulo ejecutable en la memoria persistente mutable. Cualquier instancia de la aplicación y sus datos relacionados se pueden remover. Una tarjeta Global Platform se destina a soportar varios archivos de carga ejecutables y múltiples módulos ejecutables, como múltiples aplicaciones pueden coexistir en una tarjeta Global Platform, estas actividades están representadas en la figura 24.

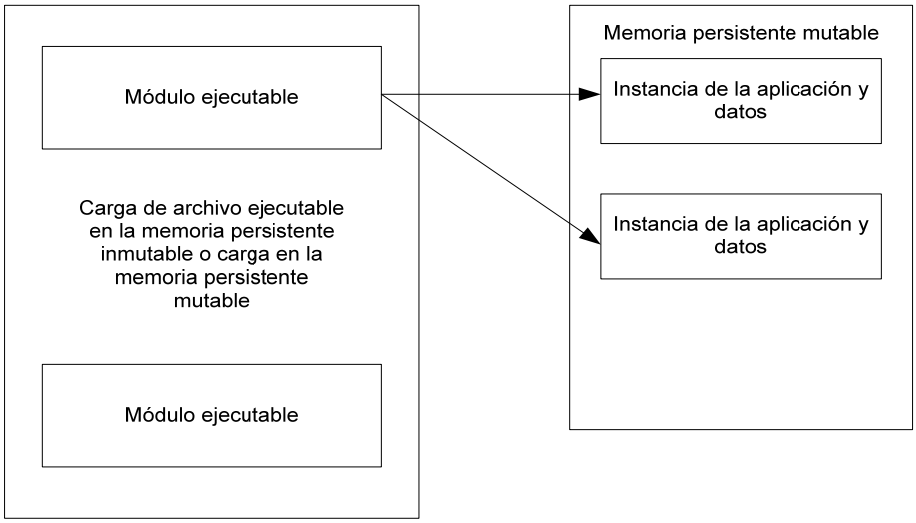


Figura 24. Carga de archivos ejecutables, un módulo ejecutable y una aplicación

En este apartado, revisamos los principales ambientes de ejecución de los sistemas operativos de las tarjetas inteligentes, enfocándonos en la arquitectura de la tarjeta según Global platform y el ambiente de ejecución de Java Card. Son fundamentales los conceptos del OPEN, de los dominios de seguridad, del Administrador de la tarjeta, por ser estas instancias donde se ejecutan las actividades de bajo nivel a través de comandos APDU, que tienen interfaz con el SGTI para la rastreabilidad y seguridad de los procesos del ciclo de vida de la tarjeta y aplicaciones.

2.8 Estándares y normas asociadas a las tarjetas inteligentes

En este capítulo se abordarán los principales estándares y normas publicados por los organismos de normalización y organismos especializados, para propiciar y mejorar la compatibilidad entre productos y favorecer la interoperabilidad de los diferentes sistemas.

Como lo señala Jack M Kaplan [R5] con base en el estándar ISO/IEC 7816-13 [W10], una característica importante que deben de cumplir las tarjetas inteligentes es su amplia compatibilidad con una gran variedad de infraestructuras informáticas. Esto es debido en parte a un gran número de normas emitidas por organismos de normalización no gubernamentales y las normas de la propia industria. Estas normas sirven como documentos base de referencia para los fabricantes de tarjetas, los desarrolladores de sistemas operativos y los desarrolladores de aplicaciones.
Las normas internacionales ISO/IEC tienen un carácter muy general con respecto a muchos de sus aspectos técnicos. Por lo tanto, son comúnmente consideradas como un marco normativo que constituye la base de las normas adicionales que exponen los detalles específicos para las aplicaciones. Estas normas adicionales,

a su vez constituyen la base de las especificaciones donde quedan claramente establecidos los detalles de implementación real.

Los grupos de la industria de las tarjetas inteligentes han desarrollado una serie de normas y especificaciones. Estas normas son voluntarias, pero generalmente son observadas en el interés de lograr la conformidad e interoperabilidad. Organizaciones de aplicaciones de sistemas basados en tarjetas inteligentes revisan las normas y especificaciones que sean pertinentes para la ejecución de las aplicaciones y determinar lo necesario para su cumplimiento.

El Government Smart Card Handbook [R2], señala que en el futuro, la práctica del uso de tarjetas inteligentes y las normas de diseño de los sistemas deben mejorar significativamente la capacidad de las normas para alcanzar los siguientes objetivos:

- Establecer una definición clara y concisa de los términos para que todos los organismos tengan un entendimiento y criterios comunes para la evaluación
- Proporcionar las normas y especificaciones que requieren las aplicaciones de las tarjetas para ser utilizadas a través de una infraestructura definida.
- Los requisitos de conducción y el reconocimiento del costo total de propiedad de una arquitectura completa del sistema
- Proporcionen la flexibilidad para satisfacer las necesidades de uso adicional de las organizaciones, así como salvaguardar el derecho del individuo a la intimidad

Un resumen de los distintos estándares, normas y especificaciones de las tarjetas inteligentes se presenta a continuación.

La Organización Internacional de Estandarización (ISO)/Comisión Electrotécnica Internacional (IEC), ISO/IEC [R3], es el organismo mundial que establece los estándares de tecnología, incluyendo los de las tarjetas de plástico. Estas normas establecen las mínimas especificaciones, pero también incluyen muchas opciones y tienden a dejar algunas cuestiones sin resolver. Como resultado de ello, la conformidad con las normas ISO/IEC por sí sola no garantiza necesariamente la interoperabilidad, ni tampoco garantiza que las tarjetas y terminales construidas con las especificaciones van a funcionar. Las principales normas que se refieren a las tarjetas inteligentes son:

ISO / IEC 7810
ISO / IEC 7811
ISO / IEC 7816,
ISO7IEC 10202
ISO / IEC 14443,
ISO / IEC 10536

ISO / IEC 10373 -1,-2,-3,-4,-5
ISO / IEC 11770
ISO / IEC 15693
ISO / IEC 7501
ISO/IEC 15448
ISO/ IEC 24727

La Norma ISO/IEC 7810, describe las características físicas generales de las tarjetas, así como el material de la tarjeta inteligente.

La norma ISO/IEC 7811 establece las especificaciones para las tarjetas de identificación, así como las características del embozamiento y de la banda magnética.

La norma ISO/IEC 7816 está dividida en catorce partes. En la parte 1 se describen las especificaciones de las características físicas de las tarjetas de circuito integrado con contactos. La parte 2 define las dimensiones y la ubicación de las áreas de acoplamiento. La parte 3 explica las señales electrónicas y los modos de transferencia. La parte 4 contiene la descripción del sistema de archivos, incluidos los tipos de archivo (MF, DF y EF), estructuras de archivos (transparente, lineal, variable lineal, cíclico y TLV-codificado), opciones de selección, los mecanismos esenciales de seguridad de la mensajería también se especifican en esta norma.

Los comandos para las operaciones criptográficas se describen en la parte 8 de la norma ISO/IEC 7816. Los comandos de administración se describen en la parte 9 de la norma ISO/IEC 7816. El protocolo USB para tarjetas inteligentes se describe en la Parte 12. En la parte 13 de la norma ISO/IEC 7816 se describe los comandos para tarjetas multiaplicativas.

Aplicaciones de firma digital para una amplia gama de tarjetas están disponibles, en el nivel de la tarjeta inteligente, el documento básico más importante es la norma ISO/IEC 7816-15, el cual se basa en el estándar PKCS # 15 generado por RSA.

La norma ISO/IEC 10202 describe los estados del ciclo de vida de tarjetas y aplicaciones, aspecto fundamental que es una de las fortalezas de las tarjetas con chip, proporciona la funcionalidad de dar seguimiento y rastreabilidad a las tarjetas y aplicaciones durante su vida útil así como de potenciar el uso de la tarjeta con actualizaciones, carga y descarga de las aplicaciones en procesos postemisión.

La norma ISO/IEC 14443 describe las normas para tarjetas de proximidad. En concreto, establece las normas para las características físicas, la energía de

radiofrecuencia y la interfaz de la señal, anticolisión y el protocolo de transmisión de las tarjetas de proximidad que operan dentro del radio de los 10 centímetros.

La norma ISO/IEC 10536 describe las normas para las características físicas, dimensiones y ubicación de las zonas de acoplamiento, y las señales electrónicas y de restablecimiento de los procedimientos.

La norma ISO/IEC 10373 establece los métodos de prueba para tarjetas de identificación y tarjetas inteligentes.

La norma ISO/IEC 11770 describe el framework y técnicas para la gestión de llaves criptográficas

La norma ISO/IEC 15693 describe las normas de las tarjetas de vecindad. En concreto, establece las normas para las características físicas, la energía de radiofrecuencia y la interfaz de la señal, anticolisión y el protocolo de transmisión para las tarjetas de proximidad que operan dentro en el radio de 1 metro

La ISO/IEC 7501 describe las normas para los documentos de uso migratorio y verificación entre países incluyendo una recomendación de la topología de las tarjetas inteligentes.

La norma ISO/IEC 15408 describe los criterios de evaluación y conformidad.

La norma ISO/IEC 24727, establece las reglas para la compatibilidad e interoperabilidad entre las aplicaciones de diferentes tarjetas y sus sistemas operativos.

Los estándares FIPS (Federal Information Processing Standards) son desarrollados por el NIST (National Institute Standards Technology), específicamente por la División de Seguridad Informática dentro del NIST. Las normas FIPS están diseñadas para proteger a los sistemas de cómputo y telecomunicaciones. Las siguientes normas FIPS se aplican a la tecnología de tarjetas inteligentes y se refieren a las normas de firma digital, estándares de cifrado avanzados y los requisitos de seguridad para módulos criptográficos.

Para firmas digitales, el estándar FIPS 186-2 especifica un conjunto de algoritmos utilizados para generar y verificar firmas digitales. Esta especificación se refiere a tres algoritmos específicamente, el algoritmo de firma digital (DSA), el algoritmo de firma digital RSA y el algoritmo de firma digital mediante curvas elípticas (ECDSA)

El estándar ANSI X9.31-1998 contiene especificaciones para el algoritmo de firma digital RSA. La norma abarca específicamente tanto la gestión manual y automatizada de llaves, utilizando tanto cifrado asimétrico y la de llave simétrica para los servicios de la industria financiera.

El estándar ANSI X9.62-1998 contiene especificaciones para el algoritmo de firma ECDSA.

Los estándares FIPS 197, para el algoritmo de cifrado avanzado (AES) especifican un algoritmo FIPS criptográfico aprobado que se puede utilizar para proteger los datos electrónicos.

Los requisitos de seguridad del estándar FIPS 140 (1-3), se refieren a las áreas relacionadas con el diseño seguro y la aplicación especifica de un módulo criptográfico: la especificación del módulo criptográfico; módulo criptográfico de puertos e interfaces, funciones, servicios de autenticación; modelo de estados finitos, la seguridad física, entorno operativo, la gestión de llaves criptográficas, la interferencia electromagnética/compatibilidad electromagnética (EMI/EMC), pruebas de auto garantía del diseño y la mitigación de ataques.

Global Platform (anteriormente Open Platform), es una organización internacional sin fines de lucro. Su objetivo es crear y promover especificaciones a nivel mundial de la tecnología de tarjetas inteligentes, incluidas las especificaciones para las tarjetas inteligentes, dispositivos de tarjetas inteligentes y los sistemas de tarjetas inteligentes.

En todo el mundo hay actualmente millones de personas que utilizan las tarjetas inteligentes que se implementan a través de especificaciones de Global Platform. Global Platform sirve a los siguientes sectores: salud, gobierno, transporte, financieros y de telecomunicaciones móviles. La estrategia de Global Platform es crear sistemas que sean interoperables, compatibles y basada en estándares.

Common Criteria (CC) se aplica a la evaluación de seguridad para productos y sistemas. El objetivo de CC es proporcionar una forma estandarizada común para evaluar los productos y servicios, lo que produce un cierto nivel de garantía para los productos y sistemas. CC fue desarrollado por organizaciones patrocinadas desde los Estados Unidos, Canadá y Europa. Estas organizaciones se reunieron y desarrollaron los criterios comunes en 1993. En 1996, se produjo Common Criteria v1.0, en 1998 se produjo v2.0, y en 1999, la versión más reciente, la versión 2.1. CC v2.1 cumple con la norma ISO/IEC 15408.

Los países del G-8 se han unido para desarrollar un formato estándar para la captura de los datos de una tarjeta de salud. Esta norma trata de establecer una interoperabilidad a través de tarjetas de salud de los países del G-8. Se dirige a los formatos de archivo, la ubicación de datos en la tarjeta, y el uso de certificados digitales para el cuidado de la salud.

Global System for Mobile Communication (GSM).GSM es un estándar para sistemas de telefonía celular, principalmente ofrecen compatibilidad internacional.

Las especificaciones vinculan un número de teléfono a la tarjeta inteligente, llamado módulo de identificación del suscriptor (SIM) o Módulo de Identidad del Usuario (UIM), en lugar de un número de teléfono. La tarjeta SIM se inserta en un teléfono para activarla.

Para agilizar la expedición de las tarjetas inteligentes interoperables a nivel mundial, Europay, Master Card y Visa (EMV) publicaron la primera versión de las especificaciones estándares para transacciones de terminales en 1995. Las especificaciones se basan en la norma ISO/IEC 7816 y sirven como una ampliación, para dar cabida a transacciones de débito y de crédito.

Una versión actualizada de esta especificación, EMV 2000 versión 4.0, se publicó en diciembre de 2000. EMV v4.0 se compone de 4 libros.

El Libro 1, de aplicación independiente del CI con la interfaz de la terminal describe los requisitos de la funcionalidad mínima requerida para el correcto funcionamiento de la interoperabilidad independiente de la aplicación a utilizar por las tarjetas de circuitos integrados y terminales.

El Libro 2, seguridad y gestión de llaves, describe la funcionalidad de seguridad mínima requerida para las tarjetas de circuitos integrados y terminales para el correcto funcionamiento y la interoperabilidad. Los requisitos y recomendaciones adicionales se proporcionan para la comunicación en línea entre el CI y el emisor y la gestión de llaves criptográficas en la terminal, el emisor y el nivel de sistema de pago.

El Libro 3, especificaciones de las aplicaciones, define los procedimientos necesarios para efectuar una transacción de los sistemas de pago entre la terminal y la tarjeta de circuitos integrados en un entorno de intercambio internacional.

El Libro 4, establece los requisitos de interfaz del titular de la tarjeta, asistente, y el comprador, se determinan las obligatorias, recomendadas y los requisitos opcionales en terminales para apoyar la aceptación de tarjetas de circuito integrado de conformidad con Libros 1, 2 y 3.

Personal Computer/Smart Card (PC/SC), grupo de trabajo para elaborar especificaciones abiertas. Este grupo ha desarrollado especificaciones abiertas para la integración de tarjetas inteligentes con las computadoras personales. Las especificaciones son independientes de la plataforma y están basados en estándares de la industria existente. Están diseñadas para permitir a los desarrolladores a crear aplicaciones de tarjetas inteligentes basadas en las aplicaciones de red segura para la banca, la atención de la salud, y el comercio electrónico. Las especificaciones incluyen la funcionalidad de cifrado y almacenamiento seguro, interfaces de programación para lectores de tarjetas

inteligentes y computadoras y una interfaz de alto nivel para el desarrollo de aplicaciones. Las especificaciones se basan en la norma ISO/IEC 7816, el estándar EMV y las normas de las aplicaciones GSM.

El marco OpenCard es un conjunto de directrices anunciadas por IBM, Netscape, NCI, y Sun Microsystems, Inc., para la integración de tarjetas inteligentes con las computadoras de la red. Las directrices se basan en estándares abiertos y proporcionan una arquitectura y un conjunto de interfaces de programación para aplicaciones (APIs) que permiten a los desarrolladores de aplicaciones y proveedores de servicios construir y desplegar soluciones de tarjetas inteligentes en cualquier computadora personal.

Mediante el uso de una tarjeta inteligente y un sistema compatible OpenCard permitirá el acceso a datos personalizados y servicios de cualquier ordenador de la red de forma dinámica para descargar de Internet todos los controladores de dispositivos que son necesarios para comunicarse con la tarjeta inteligente. Al proporcionar una interfaz de alto nivel, se pueden soportar varios tipos de tarjetas inteligentes, el marco de Open Card [W33] tiene por objeto permitir la interoperabilidad de tarjetas de proveedores independientes. El sistema incorpora el estándar de criptografía de llaves públicas (PKCS) - 11 y es extensivo a otros mecanismos de llave pública.

The Health Insurance Portability and Accountability Act (HIPAA) de 1996 (Ley Pública 104-191). Esta ley establece que la Secretaria de Salud y Servicios Humanos (HHS) de los Estados Unidos adopte normas nacionales para las aplicaciones de sistemas de transacciones electrónicas seguras de salud. Ejemplos de estas transacciones se incluyen: créditos, inscripción, requisitos, pagos, y la coordinación de las prestaciones. El objetivo de la HIPAA es crear un entorno seguro, con costo-efectivo para que las personas cumplan de manera eficiente las operaciones de atención de la salud vía electrónica.

Organización de Aviación Civil Internacional (ICAO), Directrices de Pasaportes. La ICAO es la responsable de la formulación de directrices sobre la normalización y las especificaciones de equipos emisores de documentos oficiales.

Documentos de viaje (DVLM) pasaportes, visas y documentos de viaje. Aunque las especificaciones actuales no incluyen la orientación sobre el uso de la tecnología de tarjeta inteligente, la ICAO está en el proceso de investigar la posibilidad de añadir esta funcionalidad la MRTD. ICAO ha elaborado un informe técnico sobre la posibilidad de incluir circuitos integrados con contacto en los DVLM, titulado "Uso de circuitos integrados de contacto en las máquinas de lectura de los documentos de viaje.

Para propósitos de identificación de los estándares y normas por el tipo de relación que tiene el SGTI con las tarjetas inteligentes, las clasificamos según los seis grupos siguientes, estándares y normas de:

- Especificaciones de las tarjetas inteligentes,
- Ambiente de: seguridad, aplicaciones, interoperabilidad
- Conformidad
- Procesos del ciclo de vida de las tarjetas y aplicaciones,
- Procesos específicos de operación de las tarjetas.
- Soporte de los procesos de tarjetas inteligentes

Por tanto, si tomamos como referencia las normas y estándares de mayor impacto en la industria de las tarjetas inteligentes enunciadas en [17], [18], [19], [20], [21], [22] y [R2], definimos los diccionarios de estándares asociados a tarjetas inteligentes de acuerdo a la mencionada clasificación:

2.8.1 Especificaciones de la tarjeta

Diccionario 1. Estándares de especificaciones de tarjeta

Estándar	Descripción
ISO 7810 Tarjetas de identificación, características físicas	Tarjetas de identificación, características físicas
ISO 7811 Tarjetas de identificación, técnicas de grabación	Parte 1: Embosamiento Parte 2: Banda magnética Parte 3: Ubicación de caracteres para embosamiento en tarjetas ID-1 Parte 4: Ubicación de lectura en banda magnética pistas 1 y 2 Parte 5: Ubicación de lectura escritura para banda magnética pista 3 Parte 6: Banda magnética alta coercitividad Parte 7: Banda magnética alta coercitividad, alta densidad
ISO 7812 Tarjetas de identificación	Parte 1: Sistemas de numeración para tarjetas ID Parte 2: Procedimientos de registro y aplicación
ISO 7813	Tarjetas de identificación, tarjetas de transacciones financieras
ISO/IEC 7816 Tarjetas de identificación, tarjetas de circuito integrados	Parte 1: Características físicas Parte 2: Dimensiones y ubicación de contactos Parte 3: Señales electrónicas y protocolos de transmisión

Estándar	Descripción
con contactos	Parte 4: Comandos organización seguridad Parte 5: Registro de aplicaciones de proveedores Parte 6: Elementos de datos inter industrias Parte 7: Comandos para lenguaje para tarjetas de preguntas estructuradas inter industrias Parte 8: Comandos de seguridad relacionados con inter industrias Parte 9: Comandos administración tarjeta Parte10: Respuesta de señales electrónicas para restablecer sincrónicamente tarjetas Parte 11: Verificación personal Parte 12: Interfaces USB Parte 13: Comandos tarjetas multiaplicativas Parte 15: Información de aplicaciones criptográficas basadas en PCKCS #15
ISO/IEC 10536 Tarjetas de identificación, tarjetas de circuitos integrados sin contactos	Parte 1: Características físicas Parte 2: Dimensiones y ubicaciones de las áreas de acoplamiento Parte 3: Señales electrónicas y procedimientos de restauración Parte 4: Respuesta a protocolos de transmisión y de restauración
ISO/IEC 14443 Tarjetas de identificación, tarjetas de circuitos integrados sin contactos, tarjetas de proximidad	Parte 1: Características físicas Parte 2: Potencia de radio frecuencia e interfaz de señales Parte 3: Inicialización y anticolisión Parte 4: Protocolos de transmisión
ISO/IEC 15693 Tarjetas de identificación, tarjetas de circuitos integrados sin contactos, tarjetas de vecindad	Parte 1: Características físicas Parte 2: Interfaz aérea e inicialización Parte 3: Protocolo de transmisión y anticolisión Parte 4: Conjunto de comandos extendidos y características de seguridad

2.8.2 Asociadas a ambiente de: seguridad, aplicaciones, interoperabilidad

Diccionario 2. Estándares de seguridad, aplicaciones e interoperabilidad

Estándar	Descripción
ANSI X9.84: 2001	Administración y seguridad de información biométrica
ANSI X 3.92: 1981	Algoritmos de cifrado de datos Describe el algoritmo DES

Estándar	Descripción
ANSI X 3.106: 1983	Algoritmo de cifrado de datos Modos de operación
FIPS 46-3: 1999	Estándar cifrado de datos (DES) Describe los algoritmos DES y triple DES
FIPS 74: 1981	Lineamientos para implementación y uso del estándar de cifrado NBS
FIPS 81: 1980	Modos de operación de DES
FIPS 140-2: 2001	Requerimientos de seguridad para módulos criptográficos
FIPS 180-1: 1995	Estándar de conversión (HASH) seguro (SHA-1) Describe la función hash SHA-1
FIPS 186-2: 2000	Estándar de firma digital (DDS) Describe el algoritmo DSS
FIPS 197: 2001	Estándar de cifrado avanzado (AES) Describe el algoritmo AES
IEEE 828: 1990	Estándar para la administración y configuración de planes de software
IEEE 1363: 2000	Estándar para RSA
ISO 11568 Bancos-administración de llaves	 Parte 1: Introducción a la administración de llaves Parte 2: Técnicas para administración de llaves para cifrado simétrico Parte 3: Ciclo de vida de la llave para cifrado simétrico Parte 4: Técnicas de administración de llaves para criptosistemas de llave pública Parte 5: Ciclo de vida de la llave para criptosistemas simétricos Parte 6: Esquemas de administración de llaves
Java Card 2.1: 2000 Estándar basado en Java Card. El cual es generado por el fórum Java Card y publicado por SUN MicroSystems	 API, interfaz de aplicación de programas JCRE especificación de ambiente de run time Especificación de máquina virtual de Java Card
PC/SC V1.0 Especificación de interoperabilidad para tarjetas de circuito integrado y sistemas de computadoras	Parte 1: Introducción y visIón de la arquitectura Parte 2: Requerimientos de interfaces compatibles para tarjetas de circuitos integrados y lectores

Estándar	Descripción
personales	Parte 3: Requerimientos de interfaz para PCs conectadas a dispositivos Parte 4: Consideraciones de diseño y referencia de información para diseño Parte 5: Definición del manejo de recursos de circuitos integrados Parte 6: Definición de servicios proporcionados de interface Parte 7: Dominio de aplicación y consideraciones de diseño de desarrollo Parte 8: Recomendaciones para seguridad de circuitos integrados y privacidad de dispositivos
PKCS	Estándares criptográficos de llave pública (PKCS) Estándares de la industria publicados por RSA, que focaliza en el uso de algoritmos criptográficos asimétricos
PKCS #1 V 2.1: 2001 Estándar de cifrado RSA	Describe mecanismos para cifrado y descifrado, usando algoritmo RSA
PKCS #3 V 1.4: 1993 Estándar Diffie-Hellman	Describe el mecanismo de un procedimiento de intercambio entre dos partes usando procedimiento Diffie-Hellman
PKCS #5 V 2.0: 1999	Estándar criptográfico basado en password
PKCS #11 V 2.11: 2001	Estándar criptográfico con interfaz token
PKCS #13 V 1.0: 1998	Estándar criptográfico a partir de curvas elípticas
PKCS #14 V 1.0	Estándar para la generación de números pseudo aleatorios
PKCS #15 V 1.1: 2000	Estándar formato de información criptográfico token

Estándares biométricos: Datos biométricos para los Programas de Aplicación de interfaz (BioAPI), proporciona un alto nivel genérico de modelo de autenticación biométrica. El organismo responsable del desarrollo de estándares biométricos API es el Consorcio de BioAPI. El Consorcio BioAPI se formó en 1998. En 1999, el consorcio se fusionó con el programa de autenticación de interfaz humana (HA-API). Mediante el desarrollo de una API estándar de datos biométricos, la interoperabilidad se hace posible entre una amplia gama de aplicaciones y tecnologías biométricas. BioAPI v1.1 se convirtió en un estándar ANSI, ANSI INCITS 358-2002, el 13 de febrero de 2002.

Asociación International Aerolíneas y transportación (IATA). La IATA desarrolla las normas recomendadas para las compañías aéreas y de la industria del transporte.

La IATA tiene formado un grupo de trabajo para desarrollar estándares de interoperabilidad basados en tarjetas inteligentes para boletos de viaje. Su misión es garantizar la negociación fácil y conveniente de los boletos de avión electrónicos. Además, las compañías de tarjetas de crédito como American Express, Master Card, son los grupos de apoyo para facilitar la interoperabilidad con otras empresas de la industria de viajes.

2.8.3 Procesos del ciclo de vida de las tarjetas y aplicaciones

Diccionario 3. Estándares del ciclo de vida de tarjetas y aplicaciones

Estándar	Descripción
ISO 10202-1	Ciclo de Vida de tarjetas inteligentes y aplicaciones
Global Platform Plataforma del ciclo de vida de tarjetas y aplicaciones	Especificación y perfiles de tarjetas Especificación del sistema de gestión de tarjetas inteligentes Especificación del sistema de gestión de llaves

2.8.4 Asociadas a los procesos específicos de operación de las tarjetas

Diccionario 4. Estándares de operacion de las tarjetas

Estándar	Descripción
ANSI X3.92	Especifica el algoritmo DES
ANSI X3.106	Especifica los modos del algoritmo DES
ANSI X 9.30 Criptografía llave pública usando algoritmos reversibles para la industria de servicios financieros	Parte 1: Algoritmo de firma digital (DSA) Parte 2: Algoritmo conversión (hash) seguro (SHA-1)
ANSI X 9.9	Mensajes de autenticación de instituciones financieras
ANSI X 9.17	Administración de llaves para Instituciones financieras
ANSI X 9.19	Mensajes de autenticación para Instituciones Financieras
ANSI X9.30	Estándar de la industria financiera basada en el algoritmo DSA
ANSI X 9.31	Firmas digitales usando criptografía reversible de llave pública reversible para la industria de servicios financieros
ANSI X9.42	Proyecto de normas para el acuerdo de

Estándar	Descripción
	llaves sobre la base del algoritmo Diffie-Hellman
ANSI X9.44	Proyecto de norma para el transporte de llaves basado en el algoritmo RSA
ANSI X9.55	Criptografía de llave pública para la industria de los servicios financieros: Extensión para certificados de llaves públicas y Certificados de listas de revocación para la administración de información y seguridad biométrica
EMV 2000	Especificación de tarjetas de circuitos integrados para sistemas de pagos
Libro 1 Versión 4.0: 2000	Requerimientos de la interfaz para aplicaciones independientes ICC con terminales
Libro 2 Versión 4.0: 2000	Administración de llaves y seguridad
Libro 3 Versión 4.0: 2000	Especificación de las aplicaciones
Libro 4 Versión 4.0: 2000	Requisitos de interfaz del titular de la tarjeta, el comprador y el operador
CEPS, Versión 2.1.3: 2001	Especificación conjunta para monederos electrónicos en tarjetas (derogado)
ISO 4909	Tarjetas Bancarias, contenidos de datos en banda magnética para la pista 3
ISO 8583 Mensajes originados por tarjetas de transacciones financieras especificaciones de intercambio de mensajes	Parte 1: Mensajes, elementos de datos y valores de códigos Parte 2: Procedimientos para aplicaciones y registro para códigos de identificación de instituciones Parte 3: Procedimientos de mantenimiento para mensajes, elementos de datos y valores de código
ISO 8730 Bancos, requerimientos para mensajes de autenticación	-1:1987 parte 1 DEA -2:1992 parte 2 mensajes de algoritmos de autenticación
ISO 8732	Bancos, administración de llaves
ISO 9564 Bancos, administración y seguridad del número de identificación personal (Pin)	Parte 1: Principios y técnicas para protección del Pin Parte 2: Algoritmos aprobados para cifrado del Pin Parte 3. Requerimientos de protección del Pin en operaciones fuera de línea en ATM y sistemas punto de venta
ISO 9807	Bancos y servicios financieros relacionados

Estándar	Descripción
	Requerimientos para mensajes de autenticación
ISO 9992 Tarjetas de transacciones financieras, mensajes entre tarjetas de circuitos integrados y dispositivos de aceptación de tarjetas	Parte 1: Conceptos y estructuras Parte 2: Funciones, mensajes (comandos y respuestas), elementos de datos y estructuras
ISO 10202 Tarjetas transacciones financieras-arquitectura de seguridad para sistemas de transacciones financieras usando tarjetas de circuitos integrados (retirada)	Parte 1: Ciclo de vida de la tarjeta Parte 2: Procesos transaccionales Parte 3: Relaciones de llaves criptográficas Parte 4: Módulos aplicaciones seguras Parte 5: Uso de algoritmos Parte 6: Verificación del titular de la tarjeta Parte 7: Administración de llaves Parte 8: Principios generales y vista general de tarjetas de identificación, métodos de prueba
ISO 13491 Bancos, dispositivos criptográficos seguros	Parte 1: Conceptos, requerimientos y métodos de evaluación Parte 2: lista de verificación de cumplimiento de seguridad usando sistemas de tarjeta de cinta magnética
ISO/IEC 18033 Sistemas de cifrado para la confidencialidad de la información	Parte 1: General diferencias entre algoritmos simétricos y asimétricos Parte 2: Cifrado simétrico Parte 3: Cifrado en bloque Parte 4: Cifrado en flujo
ISO 15782 Bancos, administración de certificados para servicios financieros	Parte 1: Certificados de llave pública Parte 2: Extensiones de certificados
ISO 24727 Establece las reglas para la compatibilidad e interoperabilidad entre las aplicaciones de diferentes tarjetas y sus sistemas operativos.	Parte 1: Arquitectura Parte 2: Implementación de interfaces Parte 3: Mecanismos de servicios de acceso cliente/ servidor Parte 4: Mecanismos seguros y de conectividad Parte 5: Prueba de mecanismos

2.8.5 De conformidad

Diccionario 5. Estándares de conformidad

Estándar	Descripción
Common Criteria, Versión 2.1: 1999	Idéntica a la norma ISO/IEC 15408
ISO/IEC 10373 Tarjetas de identificación, métodos de prueba	Parte 1: Pruebas de características generales Parte 2: Tarjetas con bandas magnéticas Parte 3: Tarjetas de circuitos integrados con contactos e interfaces de dispositivos relacionados Parte 4: Tarjetas de circuitos integrados sin contactos Parte 5: Tarjetas memoria óptica Parte 6: Tarjetas de proximidad Parte 7: Tarjetas de vecindad
ISO/IEC 15408 Tecnología de información, técnicas de seguridad-Common Criteria) criterios de evaluación para seguridad de TI	Parte 1: Introducción y modelo general Parte 2: Requerimientos funcionales de seguridad Parte 3: Requerimientos de aseguramiento de seguridad

2.8.6 Genéricas de soporte a tarjetas inteligentes

Diccionario 6. Estándares de soporte a tarjetas

Estándar	Descripción
ANSI / IEEE 829	Estándares para documentación de pruebas de software
ANSI / IEEE 1008	Estándar para pruebas unitarias de software
ANSI / IEEE 1012	Verificación y validación de planes de software
CCITT Z.100: 1993 CCITT	Especificación y descripción de lenguaje
ISO 639 Códigos para la representación de nombres de lenguajes	Parte 1: Códigos Alpha-2 Parte 2: Códigos Alpha-3
ISO/IEC 646 Tecnología de Información, código del conjunto de caracteres de 7	Parte 1: Códigos de países Parte 2: Sub división de códigos de países Parte 3: Códigos para nombres formales de países

Estándar	Descripción
bits ISO para intercambio de información	
ISO/IEC 9796 Tecnología de Información, técnicas de seguridad de esquemas de firmas digitales dando mensajes de recuperación	Parte 1: Mecanismos usando redundancia Parte 2: Mecanismos usando funciones hash Parte 3: Mecanismos basados en algoritmos discretos
ISO/IEC 9797 Tecnología de información-técnicas de seguridad, códigos de mensajes de autenticación (MAC)	Parte 1: Mecanismos usando cifrado en block Parte 2: Mecanismos usando una función hash dedicada
ISO/IEC 9798 Tecnología de información-técnicas de seguridad, entidades de autenticación	Parte 1: General Parte 2: Mecanismos usando algoritmos de cifrado Parte 3: Mecanismos usando técnicas de firma digital Parte 4: Mecanismos usando función de chequeo criptográfico Parte 5: Mecanismos usando técnicas de cero conocimiento Parte 6; Describe los mecanismos de autenticación basados en técnicas de transferencia manual de datos
ISO/IEC 9979	Tecnología de información, técnicas de seguridad Procedimientos para registro de algoritmos criptográficos
ISO/IEC 10116	Tecnología de información, técnicas de seguridad, modos de operación para algoritmos cifrado en bloque de n bits
ISO/IEC 10118 Tecnologías de información, técnicas de seguridad, funciones hash	Parte 1: General Parte 2: Funciones hash usando algoritmo de cifrado en bloque de n bits Parte 3: Funciones hash dedicadas Parte 4: Funciones hash usando aritmética modular
ISO/IEC 11770 Tecnología de información, técnicas de seguridad, administración de llaves	Parte 1: Marco de referencia Parte 2: Mecanismos usando técnicas simétricas Parte 3: Mecanismos usando técnicas asimétricas

Estándar	Descripción
	Parte 4: Mecanismos basados en secretos débiles
ISO/IEC 12207	Tecnología de información, procesos del ciclo de vida de software
ISO/IEC 13239	Tecnología de información, intercambio de información entre sistemas de telecomunicaciones, procedimientos bancarios de alto nivel de enlace y control (HDLC)
ISO/IEC 13888 Tecnología de información, técnicas de seguridad, no repudio	Parte 1: General Parte 2: Mecanismos usando técnicas simétricas Parte 3: Mecanismos usando técnicas asimétricas
ISO/IEC 14888 Tecnología de información, técnicas de seguridad, firma digital con apéndices	Parte 1: General Parte 2: Mecanismos basados firmas digitales Parte 3: Mecanismos basados en el problema del logaritmo discreto de un campo finito
ISO/IEC 15946 Tecnología de información, técnicas de seguridad, técnicas criptográficas basadas en curvas elípticas	Parte 1: Generales Parte 2.: Firmas digitales Parte 3: Establecimiento de llaves Parte 4: Firmas digitales dando mensajes de recuperación
ISO 17090 Infraestructura de llave pública	Parte 1: Marco de referencia y visión Parte 2: Perfil de certificado Parte 3: Políticas de administración de autoridades certificadoras
ISO/IEC 7498 Arquitectura de seguridad	Parte 1:Modelo básico Parte 2: Arquitectura de seguridad Parte 3: Nombres y direccionamiento Parte 4: Framework de administración
ISO/IEC 27001 Sistemas de Seguridad	Marco de referencia de sistemas de gestión de la seguridad

En este capítulo, se han revisado los conceptos básicos de las tarjetas inteligentes, que forman parte de los diccionarios de los perfiles de las tarjetas y de las aplicaciones, las reglas de negocios de los procesos del ciclo de vida, estructura y composición de la arquitectura de las tarjetas, así como las bases de los algoritmos de cifrado simétrico y asimétrico, todos ellos con interacción con el SGTI a través de los comandos APDU.

Capítulo 3

Componentes de un SGTI

3.1 Sistemas de información

En este capítulo abordaremos los diversos componentes que integran un sistema para la gestión de tarjetas inteligentes (SGTI). Partiremos de la base de los conceptos clásicos de sistemas de información y los correlacionaremos con los procesos del ciclo de vida de las tarjetas inteligentes, para poder establecer el marco de referencia en el cual desarrollaremos las especificaciones del mismo.

Recurriendo al enfoque que plantea Kendall & Kendal [10],

> "un sistema de información computarizado trabaja debido a la interacción resuelta entre personas y computadoras. Se requiere que las personas, los procesos, el software y el hardware trabajen al unísono".

Así también, si tomamos en cuenta el entendimiento que se tiene de un sistema de información, el cual según el diccionario Webster [W13] establece que es un:

- "Grupo de elementos independientes, pero interrelacionados que comprende un conjunto unificado,
- Instrumento que combina objetos que interactúan entre sí, diseñado para funcionar como una entidad coherente
- Conjunto de métodos
- Procedimiento o proceso para la obtención de un objetivo
- Una estructura organizada para alcanzar una visión"

Por otra parte, si nos referimos a Cuenca, Ortiz y Boza [R17], donde manifiestan

> "que hoy en día las organizaciones se enfrentan a un entorno complejo y poco estable, así como a la necesidad de mantener niveles de competitividad elevados en un mercado global".

Continuando con Cuenca [R17], que hace referencia a la empresa extendida, empresa virtual, y en general a las nuevas formas organizativas que están surgiendo,

> "entender la naturaleza y composición de las operaciones empresariales, que atraviesan los límites de la organización, se convierte en un prerrequisito para iniciar y mantener las relaciones de negocio, se hace patente el modelado de procesos de negocio para representar y entender las operaciones de la empresa".

En este contexto la relación existente entre las necesidades de información que demandan las organizaciones en ámbitos de competencia empresarial, alineamiento de procesos complejos, integración de requerimientos convergentes entre las diferentes entidades empresariales y las potencialidades que brindan los sistemas de información para dar soporte a este tipo de planteamientos, se establece la necesidad de abordar los sistemas de información bajo las condiciones requeridas por los nuevos tiempos de las necesidades organizacionales.

Como lo plantea Cuenca [R17], la integración empresarial se obtiene en términos de:

- Datos: Modelado de datos
- Organización: Modelado de sistemas y procesos
- Comunicación: Modelado de redes

Vernadat [R19] plantea, que un modelo proporciona una representación simplificada o una abstracción de la realidad; define una arquitectura como un conjunto finito de componentes interrelacionados y que una metodología es un enfoque estructurado para el seguimiento de las actividades que conducen, paso a paso, desde un sistema existente al futuro sistema teniendo en cuenta objetivos de evolución y limitaciones específicas.

De acuerdo a Cuenca [R17], para obtener la visión completa del sistema empresa en todas sus dimensiones y complejidad surge el concepto de Arquitectura de empresa.

La Arquitectura de empresa identifica los componentes principales de la organización y su relación para conseguir los objetivos de negocio. El marco de referencia o framework, es la estructura que permite almacenar y comunicar los diferentes elementos de la arquitectura de empresa.

De acuerdo con Martin [W31], una característica o un principio específico de las arquitecturas de empresa y de su marco de referencia asociado, es la definición de las vistas. La complejidad de una empresa hace que sea difícil, por no decir imposible, su estudio bajo una única perspectiva.

Normalmente no hay una única vista o capa de la arquitectura de la empresa, sino que ésta se definirá en función de las vistas que la componen.

De acuerdo a las definiciones del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE por sus siglas en inglés) en su estándar IEEE-1471-2000[R1]:

- Arquitectura: A la organización fundamental de un sistema, embebido en sus componentes, sus relaciones, sus relaciones con el ambiente y los principios de gobierno de su diseño y evolución
- Componente de arquitectura: Un documento específico, reporte, análisis, modelo u otros tangibles que contribuyen a una descripción de arquitectura
- Descripción de arquitectura: Una colección de productos para documentar una arquitectura
- Marco de referencia (framework) de arquitectura: Un estructura esquematizada que sugiere la arquitectura de componentes. Describe como estos componentes están relacionados con otros y provee definiciones genéricas para que estos componentes estén correlacionados

- Metodología arquitectural: Un término genérico que describe un enfoque estructurado para la solución de algunos o todos los problemas relacionados con la arquitectura
- Procesos de arquitectura: Una serie definida de acciones dirigidas a la meta de producir una arquitectura o una descripción de arquitectura
- Taxonomía de arquitectura: Una metodología para organizar y categorizar los artefactos arquitectónicos.
- Arquitectura empresarial: Una arquitectura en la cual el sistema en cuestión es toda la empresa, especialmente los procesos de negocio, la tecnología y sistemas de información de la organización.
- Arquitecto: El responsable del diseño y la descripción arquitectural

De acuerdo a lo anterior, podemos resumir que un sistema de información puede ser concebido como un componente de la arquitectura de empresa, a su vez que una arquitectura de empresa puede ser estudiada y desarrollada con las herramientas, metodologías y técnicas del área de conocimiento de los sistemas de información.

3.1.1 Arquitectura empresarial de información

Existen varios marcos de referencia que atienden los procesos de Arquitectura de empresa (frameworks), entre algunos otros están el de Zachman [W18], TOGAF (The Open Group Architecture Framework) [W10], y la Arquitectura Empresarial Federal de los Estados Unidos (FEA por sus siglas en inglés Federal Enterprise Architecture) [W16].

Estos marcos de referencia establecen las relaciones integrales que hay entre la razón de ser de la organización, las personas que ejecutan los procesos y la tecnología de información que la soporta, dando prioridad a la visión del negocio, es decir la tecnología y los sistemas de información como habilitadores y soporte a los procesos del negocio, según se establece en [R18].

De acuerdo al estudio realizado por Roger Sessions [R4] y publicado en [W6], los tres marcos de referencia mencionados tienen las siguientes orientaciones:

- TOGAF: A procesos de arquitectura
- Zachman: A la taxonomía de la arquitectura
- FEA: A la metodología prospectiva

El marco de referencia de Zachman está representado en la tabla 10.

Tabla 10. Matriz del marco de referencia de Zachman

Alcance	Qué Datos	Cómo Función	Dónde Lugar	Quién Personas	Cuándo Tiempo	Por qué Motivación
Visión de la organización						

Alcance	Qué Datos	Cómo Función	Dónde Lugar	Quién Personas	Cuándo Tiempo	Por qué Motivación
Modelo de negocios						
Modelo del sistema						
Modelo de tecnología						
Representación a detalle						

De acuerdo con Melissa A Cook [11], Zachman marcó la brecha, para proporcionar una metodología para controlar el caos que ocurria con los sistemas de información que se empezaron a descentralizar, cuando su propuesta fue escrita en 1987.

El marco define los diferentes niveles de abstracción de la arquitectura de información, desde el nivel más alto estratégicamente para el negocio, hasta los niveles de detalle de las operaciones, vinculando cada nivel con sus datos, sus funciones, los lugares donde ocurren los eventos, los involucrados, en qué momento y los motivos de su participación.

El marco de referencia de la Arquitectura empresarial federal de los Estados Unidos (FEA por sus siglas en inglés Federal Enterprise Architecture) [W16] está constituido por modelos de referencia correlacionados, diseñados para facilitar el análisis y la identificación de las inversiones duplicadas, diferencias y oportunidades para la colaboración dentro y através de las agencias federales.

Los modelos se describen en la tabla 11.

Tabla 11. Marco de referencia de la AEI, de la FEA

Modelo	Descripción
Referencia de negocio (BRM)	Plataforma con perspectiva funcional (substituyendo la perspectiva organizacional) de las líneas de negocio del gobierno federal, incluyendo sus operaciones internas y servicios
Referencia de desempeño (PRM)	Para medir el desempeño, su estructura expresa las relaciones causa-efecto entre salidas/entradas. Su implementación se realiza a través de una línea jerarquica; área de medición, categoría de medición, grupo e indicador
Referencia de datos (DRM)	Promueve la identificación , uso e intercambio apropiado de datos y la información, por medio de la estandarización de datos de contexto, intercambio y descripción
Referencia de aplicaciones-	Clasifica los componentes de servicio de acuerdo a cómo soportar al negocio y a los objetivos de desempeño.

Modelo	Descripción
capacidades (ARM)	Recomienda características de servicio que pueden soportar la reutilización del uso de componentes de negocios y servicios en el gobierno federal
Referencia Técnica	Categoriza los estándares y tecnologías para soportar y habilitar la entrega de los componentes de servicio y capacidades

Según TOGAF [W10], su marco de referencia está compuesto por cuatro capas arquitectónicas o vistas:

- Negocios: Describe los procesos de negocios, metas y objetivos
- Datos: Describe como los medios de almacenamiento son organizados y accesados
- Aplicaciones: Describe las aplicaciones y la forma que interactúan con otras aplicaciones
- Tecnología: Describe la infraestructura de hardware y software que soporta las aplicaciones y sus interacciones

El marco de referencia de TOGAF define arquitectura empresarial de información (AEI) como:

a. Una formal descripción de un sistema o un plan detallado del sistema al nivel de componente, para guiar su implementación (ISO/IEC 42010:2007) [W15]

b. La estructura de componentes, sus interrelaciones, los principios y guías de gobierno en su diseño y evolución en el tiempo.

El marco de referencia TOGAF, proporciona el método de desarrollo de la arquitectura (ADM por sus siglas en inglés, Architecture Development Method), el cual es el resultado de los continuos aportes de profesionales de arquitecturas empresariales, en el se describe el método para desarrollar una arquitectura empresarial, el cual constituye el núcleo de TOGAF.

Existen dos componentes principales de TOGAF, un concepto denominado Continuidad de la empresa (Enterprise Continuum) que sirve para reflejar diferentes niveles de abstracción del proceso de desarrollo de la arquitectura, donde se almacenan los diferentes recursos relevantes que se van generando, para ser utilizados en los proyectos de desarrollo de arquitectura empresarial de información y la base de recursos TOGAF estándares de base de información (SIB por sus siglas en inglés standard information base) , el cual es un conjunto de recursos, directrices, plantillas, listas de control y otros materiales en apoyo a ADM.

ADM, es un proceso iterativo y continuo entre las fases y dentro de las fases.

TOGAF, también proporciona los elementos de gobierno de la AEI, donde el gobierno se ha convertido en un requisito cada vez más visible para la gestión organizativa [R31], la adopción de gobierno en TOGAF alinea a las empresas con las mejores prácticas, asegura el nivel de visibilidad, orientación y control que apoyará todas las necesidades y sus obligaciones de los interesados en la arquitectura.

El marco de referencia de TOGAF, orientado a los procesos de arquitectura empresarial de información, señala “qué” realizar, dejando al arquitecto los “cómo” construirlos. El gobierno de la arquitectura también debe gestionarse como un proceso.

Como lo define el estándar IEEE-1471, una Arquitectura empresarial:

> “Es una arquitectura en la cual el Sistema en cuestión es toda la empresa, especialmente los procesos de negocio, la tecnología y sistemas de Información de la organización”

En este orden de ideas, exploramos que tipo de sistema representa el SGTI, las siguientes son características de su entorno y contexto:

- Sostiene involucramiento con una gran diversidad de industrias
- Existen diferentes focos de negocios entre las diferentes entidades empresariales que participan
- Tiene procesos con altos niveles de dependencia tecnológica
- Entre los participantes existen diferentes culturas tecnológicas
- Diferentes culturas de tecnología de la información
- Requiere de la integración de áreas especializadas y,
- La infraestructura tecnológica es de diversa generación y en ocasiones incompatible

En otra vertiente, las necesidades no funcionales que se requieren para un entorno de estas características:

- Alineamiento de los sistemas de información con los objetivos de los negocios
- Eliminación de redundancia no deseada de procesamiento de datos
- Aseguramiento de la calidad de la información
- Niveles de seguridad de acuerdo a los requerimientos de los procesos y de la información
- Compatibilidad, disponibilidad, veracidad y oportunidad de la información
- Neutralización de vulnerabilidades por incompatibilidad de infraestructura y,

- Necesidad de disponer de información en los niveles de competencia, operativa, táctica y ejecutiva

Por otra parte, desde un punto de vista sistémico se requieren de grandes esfuerzos para mantener el alineamiento de todos los factores que integran una organización. La entropía organizacional de una empresa por si sola ya es motivo de la implementación de varias medidas, el involucramiento de varias organizaciones en un proyecto convergente conlleva a una gran capacidad organizativa.

En resumen, concluimos que para la adopción, adquisición o desarrollo de un SGTI, se debe de considerar al grupo de industrias-empresas-especialidades que participan, como un gran sistema empresa con sus diferentes áreas de especialidad.

Derivado de lo anterior y tomando en cuenta las recomendaciones formuladas para el desarrollo de Arquitecturas empresariales como lo señala el estudio "ISO/IEC 42010:2007 Recomendaciones prácticas para describir arquitecturas de sistemas de software intensivos" [R35], podemos concluir que nuestro sistema en estudio lo abordaremos bajo un enfoque de AEI.

Avanzando en esa dirección decidimos el marco de referencia.

Teniendo como soporte la investigación sobre el comportamiento y características que guardan entre sí diferentes marcos de referencia de AEI, resumimos el estudio comparativo realizado por Roger Sessions [R4].

Característica	Zachman	TOGAF	FEA
Taxonomía completa	4	2	2
Procesos completos	1	4	2
Guías de referencia del modelo	1	3	4
Guías prácticas	1	2	2
Madurez del modelo	1	1	3
Foco de negocios	1	2	1
Guía de gobierno	1	2	3
Guía particionada	1	2	4
Catálogo predescriptivo	1	2	4
Neutralidad de vendedor	2	4	3
Información disponible	2	4	2
Tiempo de valor	1	3	1
Suma	17	31	31

Las calificaciones para cada una de las características son del 1 al 4, donde 4 es el valor máximo y 1 el valor menor.

De acuerdo a estos resultados y para los propósitos de este trabajo se consideran que las características: Procesos completos, Guías de referencia del modelo, Neutralidad de vendedor e Información disponible, tienen mayor importancia, por tanto utilizaremos el modelo de AEI de TOGAF.

Según TOGAF [W10] el desarrollo de la AEI se integra a partir de las fases descritas en la tabla 12:

Tabla 12. Fases de la AEI del marco de TOGAF

Fase	Descripción
	Preliminar
A	Visión de la Arquitectura
B	Arquitectura de negocios
C	Arquitectura del sistema de información: Arquitectura de aplicaciones y Arquitectura de datos
D	Arquitectura tecnológica
E	Oportunidades y Soluciones: Recomendaciones para implementación
F	Plan de migración
G	Gobierno de la implementación
H	Administración del cambio de la Arquitectura

3.2 Programa de tarjetas inteligentes

Podemos definir a un Programa de tarjetas inteligentes, como una iniciativa organizacional, donde la operación de sus procesos de negocio está involucrado el flujo de la información generado por las transacciones realizadas con las tarjetas inteligentes, siendo las entidades empresariales más comunes el emisor, el operador, el socio de negocios y el titular de la tarjeta.

En las organizaciones la decisión de incorporar un Programa de tarjetas inteligentes conlleva a la aceptación tácita de un cambio importante de cómo ejecutar sus procesos internos, así como de aquellos con los que tiene interrelación con otras entidades empresariales.

La definición del alcance del Programa es un factor crítico de éxito, tiene que ser precisado en términos de los servicios o procesos que se habrán de incorporar, las entidades involucradas y los roles que deberán de ejecutar, las diversas tecnologías que se deben de incluir en las tarjetas, la compatibilidad de la infraestructura tecnológica, los sistemas de soporte a la operación de las tarjetas, la capacidad de la infraestructura de terminales instalada y las aplicaciones que se deberán de desarrollar e implementar en las tarjetas.
De acuerdo a lo anterior se perfila la necesidad de disponer de sistemas especializados, tales como el propio de la gestión, la administración de las llaves

criptográficas, el sistema de colecta de transacciones electrónicas entre otros como los más importantes.

El número de participantes en un Programa de tarjetas inteligentes puede variar.

En la configuración más simple y en el caso de sistemas pequeños, los participantes suelen estar limitados al emisor de la tarjeta y a los usuarios de la tarjeta. Sistemas más grandes y complejos tienen más participantes, como el operador del sistema, el operador de la aplicación, el operador de la red, la red de negocios y los dueños o usuarios de las tarjetas.

La figura 25 muestra los participantes en un sistema habitual en el caso de los sistemas pequeños y medianos. Esto podría ser un sistema que utiliza tarjetas inteligentes, por ejemplo, tarjetas de identificación, pases de acceso o tarjetas de estacionamiento.

En tales casos, el operador genera una solicitud de emisión de la tarjeta inteligente y obtiene su tarjeta inteligente de un fabricante de tarjetas. La personalización se realiza a menudo por el fabricante de la tarjeta en estos casos, pero es ciertamente concebible que la personalización la pueda realizar el operador. El operador mantiene un servidor, para que un conjunto de terminales de tarjetas inteligentes estén conectadas a través de una red. Las tarjetas inteligentes expedidas a los usuarios se utilizan con las terminales de acuerdo con los propósitos de la aplicación. Casi todos los tipos de sistemas de tarjetas inteligentes pueden ser operados con esta configuración.

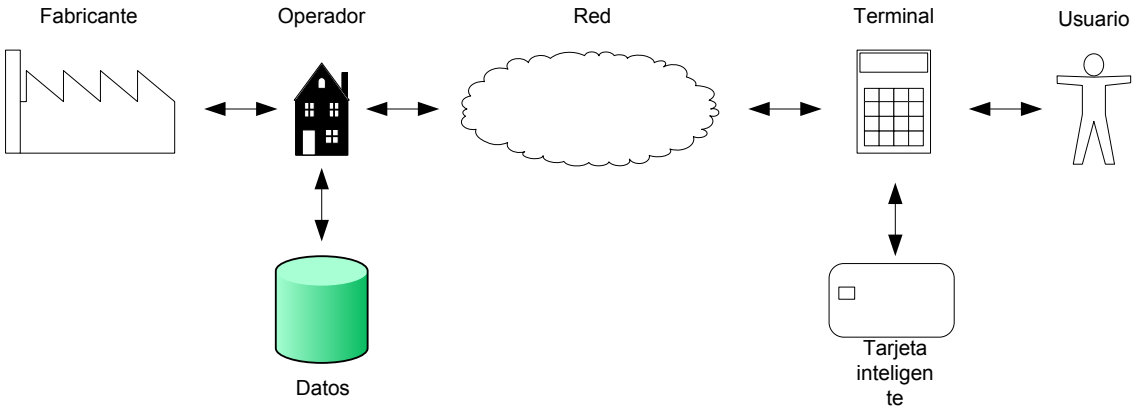


Figura 25. Ambiente de operación de un SGTI de gama media

3.3 Visión general de los sistemas de gestión de tarjetas inteligentes

Partiendo de la base de la diferencia existente entre las tarjetas de banda magnética y las tarjetas inteligentes, estableceremos las diferencias entre los requerimientos de los sistemas que las gestionan

Para la operación de las tarjetas de banda magnética, es necesario que estén enlazadas a través de sistemas de información centralizados, que les permitan gestionar sus requerimientos.

Las aplicaciones que están ligadas a las tarjetas de banda magnética, normalmente residen y se ejecutan en sistemas de información centralizados del emisor o del operador del programa, siendo la información contenida en la banda magnética la clave para la ejecución de las aplicaciones, así como los parámetros que le dan la versatilidad de que una tarjeta de este tipo pueda ejecutar varias aplicaciones.

Las características fundamentales de las tarjetas inteligentes, estriban en la incorporación de un microprocesador, capacidades de almacenamiento y recuperación de datos desde diferentes tipos de memoria (volátiles o permanentes), disposición de un sistema operativo que le proporciona funcionalidad de manejo de archivos, capacidades de gestión de la seguridad interna de la tarjeta, diferentes formas de operación de las tarjetas mediante sus interfaces de contacto o sin contacto, capacidad de ejecutar más de una aplicación y sobre todo tener el atributo de cambiar de estado en función de los eventos que ocurran a través de su operación.

De acuerdo con el Government Smart Cards Handbook [R2], un sistema de tarjetas inteligentes está integrado por cuatro componentes y su interacción:

- La tarjeta inteligente
- Las llaves
- Las aplicaciones y,
- Las transacciones

En el uso de la tarjeta inteligente, las llaves son el elemento que permite identificar plenamente a los involucrados en la operación de la tarjeta, autorizando en su caso el acceso a las aplicaciones y los datos contenidos en ella. A partir de esta acción se generan las transacciones que modifican el estado de la tarjeta y los datos asociados al sistema.

Timothy Jurguensen [21] refiere que un sistema de gestión de tarjetas inteligentes, está conformado por un subsistema de emisión y cuatro componentes:

El subsistema de emisión está compuesto por:

- Módulo de captura de datos
- Servicios de impresión de tarjetas
- Procesos de personalización de las tarjetas y,
- Procesos para el manejo de información biométrica y captura de fotografías

Los cuatro componentes son:

- Autoridad certificadora: Responsable de la emisión de los certificados de firma digital
- Servicios de directorio: Soporte para solventar las funcionalidades de PKI, confirmación en tiempo real y listas de revocación de certificados, cómo lo señala Austin [7]
- Administrador de llaves: Sistema creador, generador y gestor de las llaves que se emplean en la tarjeta
- Administrador de aplicaciones: Instancia para vincular correctamente las aplicaciones que están en la tarjeta o detectar las aplicaciones que deben de estar en la tarjeta

Global Platform [W7] establece que el ambiente de un sistema de gestión de tarjetas inteligentes deberá de incluir funcionalidad en cinco áreas:

- Definición y mantenimiento del portafolio: Es el proceso requerido para mantener actualizados los perfiles de las tarjetas y aplicaciones, configurar el portafolio de productos y preparar los componentes necesarios del ambiente para estar en condiciones de emitir las tarjetas
- Emisión de tarjetas: La colección y preparación de los perfiles de tarjetas y aplicaciones, comandos, datos y llaves necesarias para habilitar y personalizar tarjetas con multiaplicaciones
- Mantenimiento de tarjetas y aplicaciones: La administración y mantenimiento de todas las tarjetas de manera individual y sus aplicaciones, las cuales incluyen registrar y almacenar los cambios en los estados de su ciclo de vida
- Descarga de aplicaciones: La posibilidad de agregar , actualizar o borrar aplicaciones en fase de postemisión
- Requerimientos de distribución: La posibilidad de soportar múltiples aplicaciones de múltiples proveedores

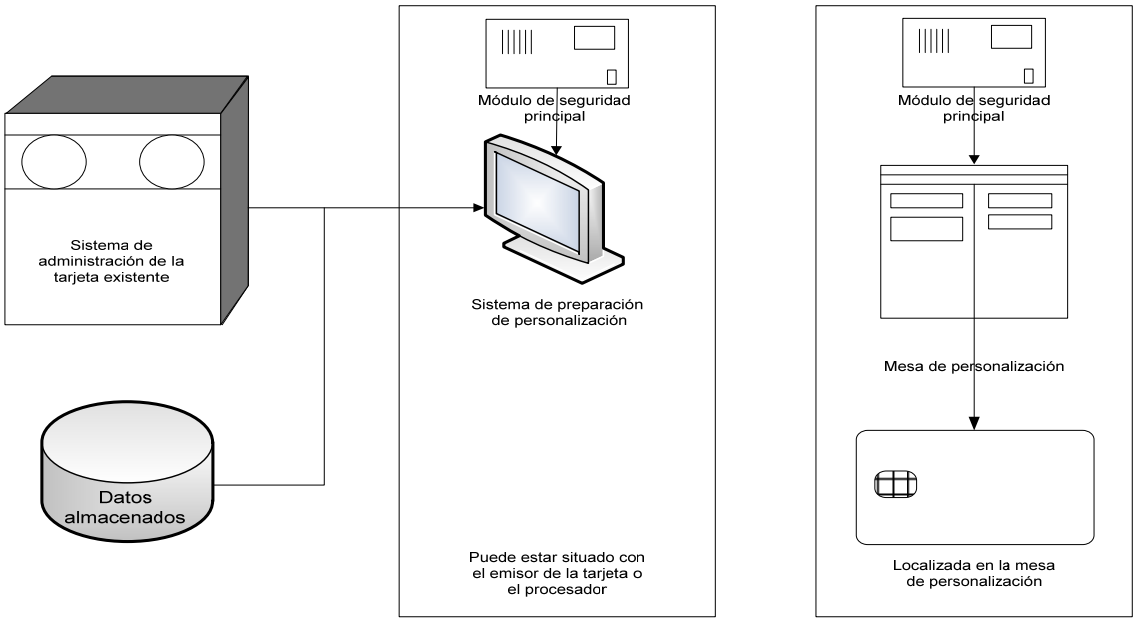
La figura 26 muestra el flujo de un sistema para la preparación de la personalización de tarjetas.

Abundando en lo anterior, la visión que expone Mike Hendry [19] con respecto a los sistemas de gestión de tarjetas de otras tecnologías, que migran al ambiente de tarjetas inteligentes, resalta lo siguiente:

- Aprovechamiento de la información de los sistemas legados, aspecto importante, puesto que uno de los principales costos y factor crítico de éxito en la construcción de un SGTI es la presencia física de los titulares para la captura de su información. Esta actividad implica procesos de migración de ambientes de datos, desde archivos planos o indexados hacia ambientes de administradores de bases de datos relacionales

- Seguimiento de las tarjetas que se hayan expedido, sus fechas de expiración, las aplicaciones que se hayan instalado, las versiones de las aplicaciones y los diversos eventos ocurridos durante su vida útil

- Para aplicaciones como la emisión de tarjetas de crédito, el SGTI puede enlazar a otros sistemas, tales como un sistema de autorización, al del centro de llamadas, reportes y manejo de listas calientes



Sistema de preparación de la personalización.

Figura 26. Sistema para la preparación de la personalización de tarjetas

Cuando la tarjeta se vincula a un sistema de gestión en línea, la base de datos de las transacciones está en línea (para los propósitos de autenticación o de autorización), este vínculo es más complejo, ya que la tarjeta puede contener datos variables: un contador de transacción, o un registro de los datos almacenados por las transacciones fuera de línea. Se pueden almacenar estos

campos adicionales en el sistema de gestión de tarjetas o almacenar un apuntador a la transacción más reciente o a otro registro de datos.

Muchas de las tarjetas inteligentes, a través del sistema operativo, utilizan secuencias de comandos para actualizar los parámetros de la tarjeta.

Estos mensajes deben ser muy cortos, de modo que no exista ningún retraso en la transacción, pero que permita que la tarjeta actualice uno o más campos en su memoria, como se lo instruye el anfitrión. El sistema de mensajería debe ser seguro, por lo que las terminales no pueden ser suplantadas, interceptadas o enviar "mensajes" para modificar el valor de los saldos o los límites autorizados de las tarjetas.

Existen fuera de la plataforma, productos disponibles para la manipulación de la secuencia de comandos, que son diseñados para reducir al mínimo los cambios necesarios del SGTI y los sistemas de autorización.

El SGTI puede llamar a la secuencia de comandos del sistema de tratamiento como parte de su procesamiento de transacciones, o puede contener una bandera para indicar que una secuencia de comandos está pendiente de atender para dicha tarjeta.

El sistema de manejo de secuencias de comandos, véase la figura 27, almacena las secuencias de comandos estándar y permiten que nuevos scripts se generen.

Los guiones pueden ser programados, ya sea como resultado directo de una transacción por ejemplo, un cambio de Pin o de la carga de valor o por un sistema de procesamiento por lotes. El manejo de secuencias de comandos del sistema completo tiene la cobertura desde la entrega de secuencias de comandos, pasando por la anulación de una secuencia de comandos programados de la siguiente transacción, hasta cuando se confirma que la entrega fue un éxito.

Los beneficios de la utilización de tarjetas inteligentes (en lugar de banda magnética y de tecnologías solamente de lectura, tales como códigos de barras) son disponer de su capacidad para almacenar datos que no sólo varían de un usuario a otro, sino también que evolucionan con el tiempo. Esto es potencialmente de gran beneficio para la gestión de relaciones con clientes (teniendo en cuenta las transacciones anteriores, la historia en el procesamiento de la transacción actual) y para el desarrollo de un segmento de enfoque de mercadotecnia uno a uno (ya que permite que los productos y los mensajes se adapten al cliente en particular).

Para los casos de extravió o robo de una tarjeta, mediante una solicitud, un SGTI debe de ser capaz de emitir una nueva tarjeta, con el mismo estado en que se

encontraba la reportada, tanto en la versión de las aplicaciones como los valores almacenados en ellas.

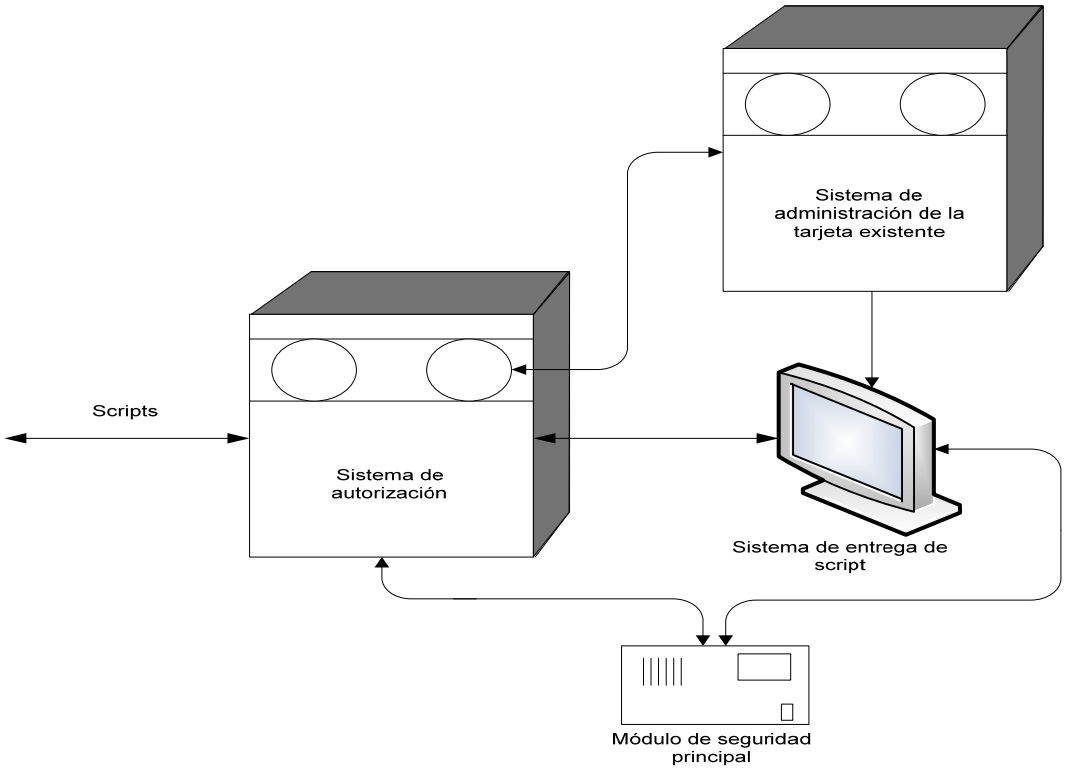


Figura 27. Entrega de scripts

Tener varias aplicaciones estáticas en una tarjeta no suele aumentar significativamente la complejidad, las solicitudes deben tener la misma fecha de vencimiento. Típicamente cada aplicación gestiona sus propios datos, las transacciones son enviadas a los diferentes sistemas en una fase temprana a un sistema de conmutación en la terminal o la red. Algunas veces una terminal generará dos mensajes durante una operación subyacente, por ejemplo, una para el pago y otro para los puntos de lealtad, tiempo aire de teléfonos móviles o de verificación de pertenencia, véase la figura 28.

La complejidad aumenta significativamente, sin embargo, si las aplicaciones son propias o desarrolladas por diferentes organizaciones, o si hay implicaciones comerciales o de responsabilidad que cruzan las fronteras de la organización. Por ejemplo, si una tarjeta contiene una aplicación de transporte y la aplicación de un crédito de tarjetas de pago, si el titular de la tarjeta no resuelve la factura de la tarjeta de crédito, el banco tendrá que bloquear la tarjeta, e incluso pueden retener

la tarjeta si se opera en un cajero automático. Esto requiere que las aplicaciones sean bloqueadas por separado. Sin embargo, si el cliente informa que la tarjeta fue robada, entonces ambas aplicaciones y la tarjeta se deben de bloquear lo antes posible, independientemente de quien maneje el informe de la pérdida.

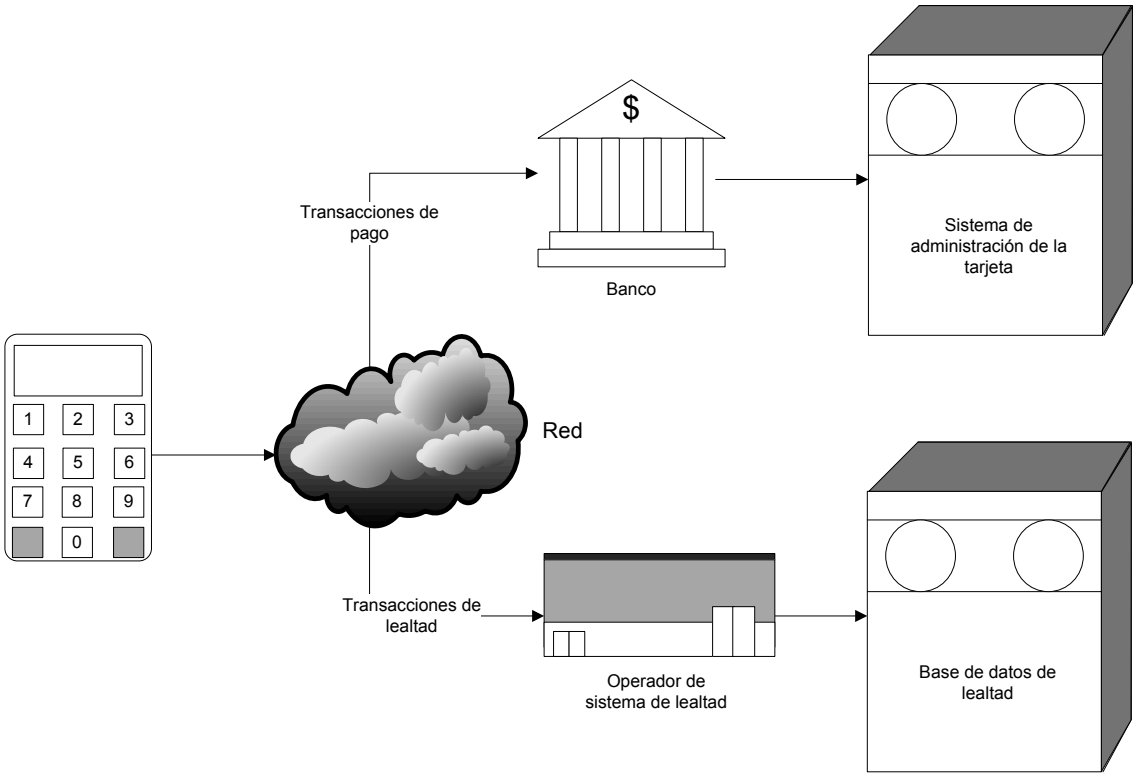


Figura 28. Enrutamiento de múltiples tipos de transacciones

Los sistemas de gestión de tarjetas inteligentes se diseñan para manejar estas situaciones y pueden incluir interfaces para más de un centro de llamadas con diferentes responsabilidades y derechos.

No siempre es posible cargar todas las aplicaciones en el momento de la personalización inicial, a veces las aplicaciones principales se almacenan en ROM, pero aplicaciones adicionales (dependiendo del perfil del titular de la tarjeta) se pueden cargar antes o después de que la tarjeta es emitida al titular.

Cualquiera de estas situaciones, donde algunas de las aplicaciones se puede considerar "en vivo", deben ser tratadas como un proceso de postemisión desde el punto de vista de la seguridad. Una tarjeta que ofrece la facilidad de descargar

aplicaciones postemisión es una herramienta mucho más flexible para el emisor, y puede ahorrar costos considerables si existen cambios de las necesidades durante la vida de la tarjeta. Aquí, hay un requisito no sólo para asegurar que todas las aplicaciones sean instaladas en su estado correcto cuando una tarjeta es reemitida, sino también para gestionar el proceso de la descarga en sí mismo, para autenticar las aplicaciones descargadas y para garantizar que se cargan en un espacio de memoria adecuado en la tarjeta.

Tanto Global Platform como Java Card o Multos hacen hincapié en este aspecto, ellos tienen las especificaciones para la gestión de tarjetas inteligentes que complementan las especificaciones de la tarjeta. Una parte importante de esto es la capacidad de la tarjeta para reconocer una solicitud aprobada para su descarga, lo que requiere una estructura de gestión de llaves que permite al emisor de la aplicación mostrar que la solicitud es auténtica y ha sido certificado por el emisor de la tarjeta.

Si se utiliza una estructura de llave simétrica, entonces es probable que el sistema de gestión de la tarjeta tendrá que desempeñar un papel en dicha estructura (la llave pública del emisor de la tarjeta puede ser almacenada en la tarjeta para verificación de los certificados de carga de aplicación). El sistema de gestión de las tarjetas también debe dar seguimiento de la memoria disponible en la tarjeta, teniendo en cuenta la necesidad de almacenamiento temporal durante la descarga y el proceso de descifrado.

Un SGTI es esencial para la gestión de la descarga en postemisión, si las solicitudes se añadirán a la tarjeta después de que se haya expedido, si las solicitudes tienen cambios sustanciales durante la vida de la tarjeta, o si queremos la capacidad de volver a emitir una tarjeta que contiene múltiples aplicaciones dinámicas, entonces un SGTI deberá de gestionar la complejidad de cualquier conjunto de subsistemas.

Una tarjeta inteligente es un sistema informático que pasa por varios estados, desde el primero, en la creación de un circuito integrado con una máscara hasta las etapas de la personalización, expedición, bloqueo y desbloqueo, y, finalmente, expiración y destrucción. Como vemos en la figura 29, las aplicaciones en la tarjeta pasan por una versión abreviada de este ciclo, no necesariamente en el mismo plazo. (Lo único que siempre se debe evitar es tener una aplicación en una tarjeta con fecha de vencimiento posterior que el de la propia tarjeta, o de cualquier aplicación maestra).

Durante el proceso de producción de las tarjetas, la tarjeta pasa por una secuencia de pruebas, de la escritura del chip y los datos del fabricante de la tarjeta, y, finalmente, la personalización. En el final de cada etapa, un bloqueo irreversible es ejecutado, y la tarjeta pasa a un nuevo estatus. Dependiendo de la relación con el proveedor de la personalización de tarjetas, puede ser necesario que el emisor

almacene los datos relacionados con la producción de datos tales como números de tarjeta y versión de software, lotes, fechas de congelación de los cambios, el envío de fechas o identificadores de llave para los archivos de personalización. Estos datos pueden estar disponibles en el centro de llamadas o para volver a los sistemas de expedición, lo que permite búsquedas más complejas para ser contestadas o tarjetas para ser reemitidas en intervalos muy cortos. Esto exige un intercambio de datos con el sistema de personalización.

El sistema de gestión de tarjetas inteligentes da pistas de estas etapas del ciclo de vida y avisa al emisor cuando hay algún conflicto o cuando hay que tomar medidas para restaurar una tarjeta a un estado operacional.

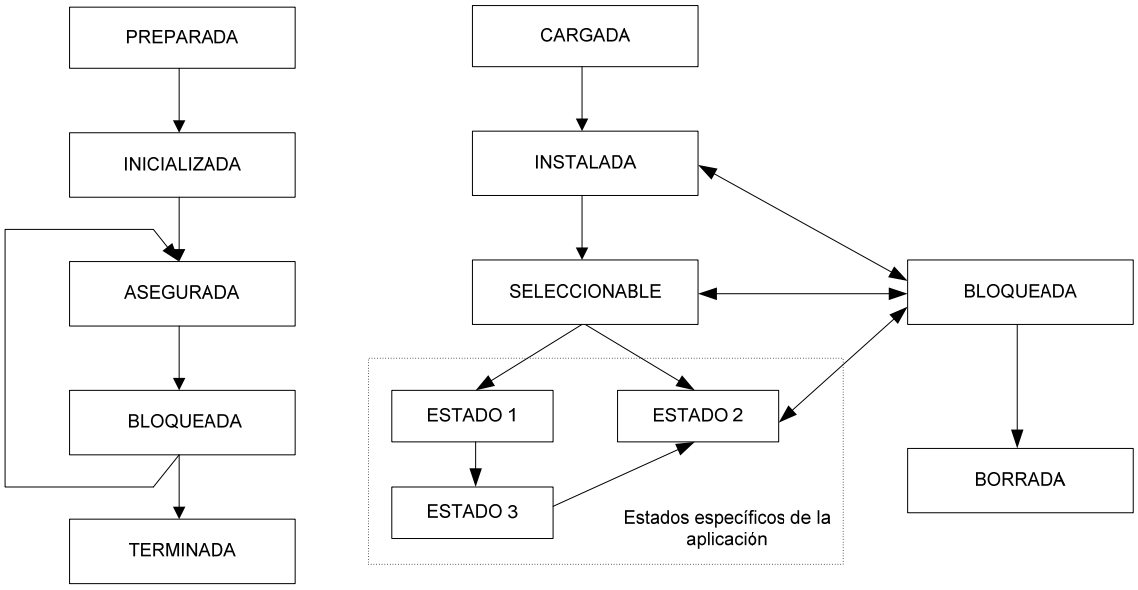


Figura 29. Ciclo de vida de las aplicaciones y de la tarjeta

Los sistemas de gestión de tarjetas inteligentes no han sido ampliamente desplegados por los bancos o emisores de tarjetas para el transporte público, y gran parte de la experiencia en este campo proviene de sectores tales como la tarjeta de identificación corporativa, el gobierno y las industrias de telefonía móvil.

La mayoría del software de un SGTI es desarrollado dentro de uno u otro de estos sectores, y posteriormente generalizado para los demás sectores. Así que lo primero es garantizar que el sistema es totalmente "consciente" de las necesidades específicas y las estructuras de los sectores en los que será utilizado. Se debe interactuar con todos los sistemas relevantes de los

registros de los clientes, sistemas de tratamiento en tiempo real, con los canales de distribución y los servidores de sistemas.

A través de un portafolio de productos de tarjeta, las relaciones entre las tarjetas, los titulares de las tarjetas, las cuentas y los titulares de cuentas, pueden ser bastante complejas. La complejidad aumenta si tenemos en cuenta las solicitudes, las llaves, los parámetros dentro de la tarjeta, otras aplicaciones y, en particular, los propietarios de cualquier aplicación externa.

También es importante ser capaz de definir los usos a los que el SGTI será destinado, lo que necesitamos, por ejemplo, para gestionar las aplicaciones externas o múltiples aplicaciones de autoridades de certificación ? descargar aplicaciones de manera regular o simplemente que sea un requisito de vez en cuando? ¿Con qué bases de datos debemos interactuar? ¿Qué parámetros se establecerán de forma individual para la tarjeta o tarjetas base de titulares y si estos se ajustarán de forma automática o manualmente? Estas son las respuestas que pueden afectar no sólo la configuración de los SGTI, sino incluso su selección.

Uno de los beneficios de un sistema de tarjetas multiaplicación es la flexibilidad para ampliar su funcionalidad poco a poco, cuando se emiten las primeras tarjetas, la estructura final completa puede no ser conocida y por lo tanto es difícil responder a estas preguntas.

Por otro lado, es importante implantar un SGTI antes que la gestión del ciclo se vuelva demasiado compleja, en otras palabras, debe aplicarse antes de que sea necesario. Para hacer frente a esto, muchos SGTI operan en "situación progresiva" de acuerdo a características o acuerdos de licencia, lo que significa que pueden llevarse a cabo en fases.

Por último, la gestión del SGTI debe ser planificada y diseñada. Esto puede ser una actividad operativa importante, que requiere conocimientos especializados de la tarjeta y la tecnología de software, los requisitos de negocio y de los socios o la gestión de canales.

En resumen, las funcionalidades que debe de cumplir un SGTI son:

- Almacenamiento en los campos de la tarjeta, de datos específicos, incluidos los campos que se actualizan dinámicamente con la operación del sistema en tiempo real de procesamiento
- Manejo de secuencias de comandos para los cambios de parámetros
- Descargar y actualizar las solicitudes de tarjeta
- Almacenamiento de datos para múltiples aplicaciones
- Almacenamiento de datos de producción y volver a la tarjeta datos de emisión

- Gestión del ciclo de vida a través de la creación, emisión, aplicación o el bloqueo de la tarjeta, de caducidad, por extravió u robo
- Gestión de llaves públicas y el módulo de hardware seguro (HSM por sus siglas en inglés) para la gestión de llaves simétricas y la generación de certificados
- Soporte de biometría (registro, almacenamiento de plantilla)
- Gestión de los inventarios
- Producción en pequeños volúmenes y la expedición de emergencia y,
- Generación de pistas de auditoría e informes de gestión

Este conjunto de funciones permite a un SGTI volver a emitir una tarjeta que se ve casi idéntica a la original, sin la necesidad de integrar varios subsistemas de nuevo. Hay muchas interfaces externas, el esfuerzo de integración inicial es aún significativo, pero los cambios y las actualizaciones son más fáciles de lograr con un SGTI que con un sistema legado o la integración de varios subsistemas.

Muchos sectores tienen requerimientos específicos, los bancos necesitan el apoyo de las especificaciones EMV y de sistemas de gestión del riesgo, deben también cumplir con el pago a la industria de las tarjetas para los requisitos de seguridad de los datos almacenados y transacciones, y para el acceso a los datos de la tarjeta. Muchos operadores de transporte deberán tener el apoyo de MiFare [W38], FeliCa [W39].

Los proyectos de tarjetas del gobierno pueden requerir una amplia gama de interfaces para diferentes departamentos, cada uno con sus propios derechos de acceso y requisitos de seguridad. Algunas aplicaciones requieren la certificación para un sistema de tarjeta o de un laboratorio de seguridad.

La mayoría de los proveedores desarrollan sus primeros productos para satisfacer las necesidades específicas de un sector, y luego ampliar las funciones para cubrir las necesidades de otros sectores. Por esta razón, es importante garantizar que las funciones de un sistema que se está comprando cubra toda la gama de necesidades probables durante la vida útil del sistema, o pueda ser fácilmente extendido y certificado.

Global Platform publica un amplio conjunto de requisitos funcionales para un SGTI, aunque no es una especificación completa, describe los componentes y las funciones necesaria para gestionar cualquier tarjeta Global Platform o las aplicaciones, a través de su ciclo de vida. Muchos de los productos SGTI (sean o no certificados conformes) son compatibles con Global Platform y Multos para los protocolos de carga y de eliminación de aplicaciones.

Una visión importante que aporta Global Platform [W7] con respecto a la funcionalidad de un SGTI, es la definición, descripción, relación y rol que tienen

cada uno de las diferentes entidades empresariales que participan durante el ciclo de vida de una tarjeta inteligente y sus aplicaciones.

Hay varios actores involucrados en la producción, distribución y mantenimiento de un programa de multiaplicaciones para tarjetas inteligentes. La figura 30 proporciona una visón del ambiente GP de alto nivel, que muestra las interrelaciones de varios roles. Es entendido únicamente como una referencia de alto nivel; descripciones de más detalle están contenidas en la definición de las especificaciones.

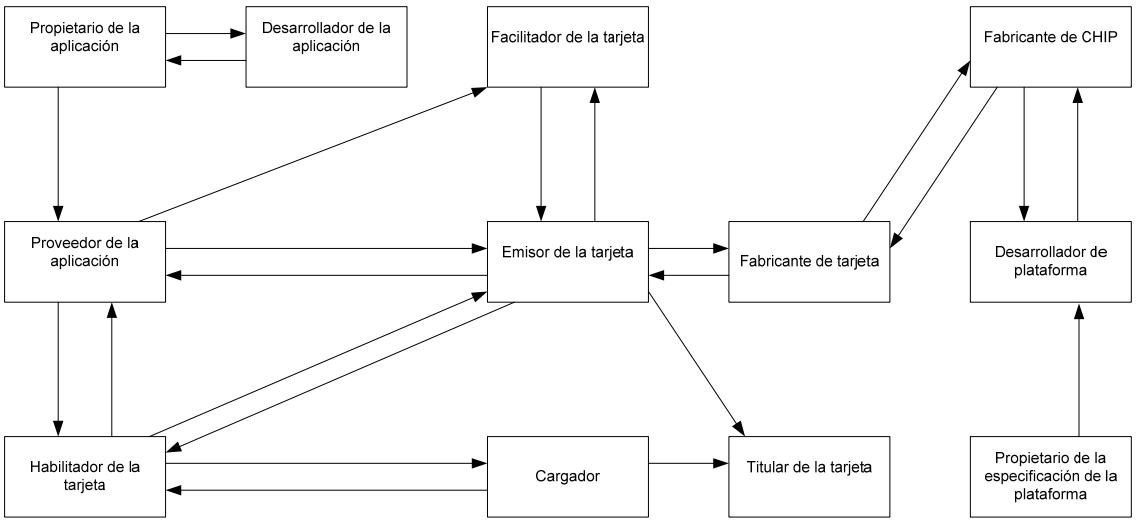


Figura 30. Interelación de entidades empresariales en un ambiente de tarjetas

Otro aspecto importante a considerar en la funcionalidad del SGTI es su ambiente de operación.

La premisa en un Programa de tarjetas, donde están todas las entidades empresariales, involucrados y roles implicados, es la seguridad que debe de prevalecer en los componentes y en la información contenida.

Las alternativas del ambiente son operación centralizada y descentralizada. Hay actividades que por la naturaleza de su función sólo pueden realizarse de una manera, algunas otras tienen la opción de realizarse de cualquiera de las dos modalidades, como es el caso de la carga/descarga de aplicaciones en postemisión.

La gestión de una tarjeta inteligente y sus aplicaciones requieren varios componentes de sistemas de soporte interno (back office). Ciertos componentes están relacionados con la producción de la tarjeta, otros con la gestión del ciclo de vida y otros están relacionados con las aplicaciones. Típicamente el ambiente del

SGTI tiene interfaz entre un sistema principal y sistemas legados de un emisor y con sistemas de tercera parte de proveedores de servicios y aplicaciones.

En el caso de un ambiente distribuido, los componentes de sistemas individuales pueden ser proporcionados por entidades empresariales separadas y usadas en diferentes formas dependiendo de los requerimientos del emisor de la tarjeta y el estado de producción de la tarjeta.

Contemplemos esta situación, los procesos relacionados de producción de la tarjeta para emisión inicial, carga de aplicaciones y personalización en postemisión tienen algunos datos comunes que aunque se necesitan pueden ser procesados por entidades empresariales separadas. La inicialización de las tarjetas y procesos de descarga en postemisión pueden tener algunos procedimientos reutilizables, los cuales pueden ser ejecutados por el mismo sistema.

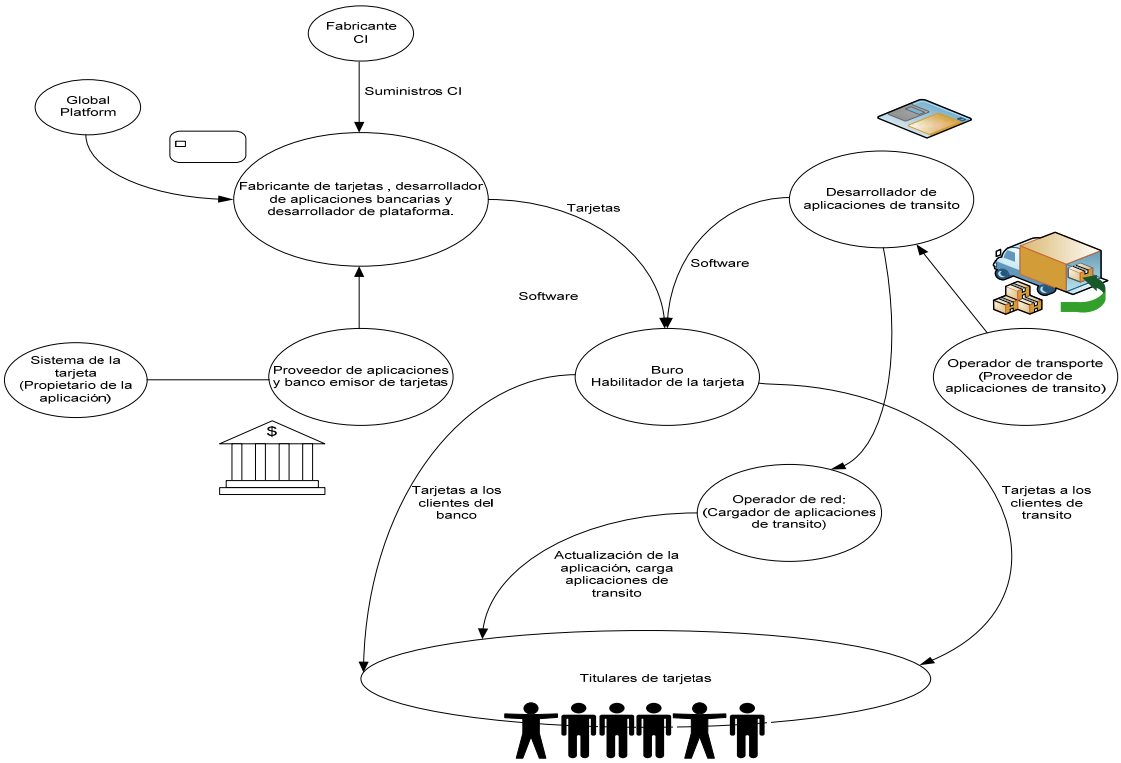


Figura 31. Ambiente de operación entre varias entidades y multiaplicaciones

Puede ser el caso, sin embargo, que el rendimiento tenga limitaciones en un ambiente de postemisión, se puede necesitar que los procedimientos sean replicados en un ambiente de postemisión por ambas entidades empresariales, las que preparan los datos para la producción de la tarjeta y la entidad que ejecuta la descarga de las aplicaciones en postemisión.

La clave de la arquitectura de un ambiente SGTI es el reconocimiento de los roles que desempeñan las diferentes partes en un entorno multiaplicación.

Considerando que para una aplicación única, la tarjeta puede, en principio, aceptar que el emisor de la tarjeta asuma la responsabilidad de todos los aspectos del desarrollo de la tarjeta, la producción y uso, para una tarjeta multiaplicación, hay un conjunto complejo de relaciones entre los desarrolladores, implementadores y los usuarios operativos de la tarjeta.

La figura 31 muestra un ejemplo de la forma en que pueden interactuar diversas entidades empresariales en un programa de tarjetas inteligentes.

3.4 Procesos para la preparación de datos

Como se describió en el apartado 2.5.2.3 de este trabajo, durante la tercera fase del ciclo de vida de las tarjetas, se realiza la personalización gráfica y eléctrica de las tarjetas.

Así también se refirió en el apartado 2.7.2.3, que es en los dominios de seguridad donde se cargan las aplicaciones vía el Administrador de la tarjeta.

Con respecto a los datos que deberán de ser cargados en su respectivo dominio en la tarjeta, se deben de realizar actividades que garanticen la integridad de los mismos, la compatibilidad de los datos con las aplicaciones que los emplearan y el tamaño del espacio en EEPROM donde se almacenaran, entre otras.

Para tal efecto hay que realizar el mapeo (conocido en el mercado como mapping del chip) de las estructuras de datos del mundo externo hacia las estructuras de datos de los archivos de la tarjeta.

Tomando en cuenta los sistemas de información, donde se contienen los datos fuente, las bases de datos que se hayan almacenado con los datos de los titulares de las tarjetas, clientes y entidades empresariales involucradas en las aplicaciones, se deberán de realizar procesos para lograr la integridad y calidad de los datos a migrar a las tarjetas.

Todas las actividades de integración, migración de ambientes de bases de datos y la definición de la exportación hacia los medios de almacenamiento que físicamente entregarán los datos a los equipos de personalización, deberán de realizarse en un ambiente que gestione la seguridad de la Información.

Como premisa gran parte del éxito de un Programa de tarjetas Inteligentes tiene que estar relacionado con la seguridad y la calidad de los datos que se incorporan. Hay costos de oportunidad de los datos, que son la consecuencia de tener la posibilidad que una sola vez el titular de la tarjeta esté presente en la actividad del

enrolamiento o en el requisitado de los formatos para capturar sus datos, lo que es el inicio de las actividades del procesamiento de datos.

Las fortalezas de las tarjetas inteligentes son la: seguridad, confiabilidad, integridad, disponibilidad, movilidad y confidencialidad con que se manejen los datos de los titulares y entidades empresariales involucradas, por estas razones es necesario la implementación de procesos de calidad de datos para alcanzar los objetivos.

Las dos vertientes que existen cuando se van a integrar los datos del mundo externo a las tarjetas son en primera instancia datos que existen en bases de datos legadas en los diferentes sistemas que integran el SGTI, la segunda es cuando se van a crear a partir de algún programa específico de captura de los datos.
En ambos casos los procesos de calidad de los datos deben de estar presentes, para el primer caso, puede suceder que se tengan que realizar procesos de transformación a nuevos formatos, exportación o migración hacia ambientes tecnológicamente más actualizados o en el caso extremo diseñar y ejecutar un programa de limpieza y consistencia de datos.

Conforme a esta necesidad y de acuerdo con Piattini [8] y Huang K.T [24]

> "las empresas deben de gestionar la información como un producto importante, capitalizar el conocimiento como un activo principal y de esta manera, sobrevivir y prosperar en la economía digital".

La calidad de la información producida está en función de dos componentes: la calidad del sistema de información que procesa los datos y la calidad de los datos, una impacta a la otra.

En este contexto y tomando como referencia a Piattini [8], señala que la calidad de la información está estructurada según se muestra en la tabla 13.

Tabla 13. Estructura de la calidad de la información

Calidad de la información		
a) Calidad de la base de datos	a1) Calidad del sistema de gestión de la base de datos (SGBD)	
	a2) Calidad del Modelo de Datos	a2.1) Calidad del Modelo conceptual a2.2) Calidad del Modelo lógico

Calidad de la información		
		a2.3) Calidad del Modelo físico
	a3) Calidad de los Datos	a3.1) Cumplimiento de las especificaciones, valores y validaciones
b) Calidad del sistema de información	Cumplimiento de las especificaciones	

La calidad del SGBD, está asociada al ambiente de operación de la base de datos, la selección del mismo está en función de características tecnológicas y de soporte de los productos que presente el mercado, de la compatibilidad con la infraestructura tecnológica que se disponga, de la experiencia y capacitación del personal que la administre, de las medidas de seguridad que sea necesario implementar con base en un análisis de riesgos de la información, de la administración de la demanda, de la administración de las capacidades, de la administración de incidentes y problemas; y de la administración de los planes de continuidad del negocio.

La calidad del modelo conceptual está compuesto por dos vertientes: la calidad del producto y la calidad del proceso.

La calidad del producto está relacionada con las características del modelo conceptual y la calidad del proceso en como se desarrollan los modelos conceptuales.

Una propuesta de metodología y métricas para evaluar la calidad del modelo entidad/relación (E/R) la presenta Kesh [25], que considera dos tipos de componentes: de comportamiento y ontológicos.

Los modelos E/R están formados por dos componentes ontológicos: la estructura y el contenido. La estructura tiene que ver con las entidades y sus relaciones y el contenido se refiere a los atributos de las entidades. La tabla 14 muestra los factores que influyen en la calidad de los modelo E/R.

Tabla 14. Factores que influyen en la calidad de los modelos entidad/relación

- Componentes de comportamiento:
    - Mantenibilidad: Es la facilidad con que un diagrama E/R puede ser modificado, corregido y extendido ante futuros requerimientos
    - Precisión: A la exactitud con que el diagrama E/R refleja el problema que se está modelando
    - Rendimiento: En el diseño eficiente del diagrama E/R, la eficiencia es el número de entidades, relaciones y atributos con relación al tipo de tarea que la base de datos representa
    - Usabilidad: Si un diagrama E/R es conveniente y práctico para su uso, del usuario y del diseñador

- Componentes ontológicos:
    - Estructura
        - Adecuación al problema: Se refiere si el diseño del modelo E/R refleja la estructura del problema que se está modelando
        - Concisión: El modelo no tenga redundancia no deseada
        - Consistencia: El modelo no muestre contradicciones
        - Validez: Cumplimiento de principios técnicos de diseño
    - Contenido
        - Cohesión: A la cercanía entre los atributos de una entidad
        - Compleción: Todos los atributos relevantes deben ser incluidos
        - Validez: Los atributos sean correctamente asignados a las entidades

En términos de lo anterior, siguiendo con Piattini [8] y de acuerdo en lo que señala el estándar ISO 9126 (Estándar para la evaluación de calidad del software), tres de los factores que influyen en el mantenimiento son: el análisis, los cambios y la facilidad de prueba.

En atención a la solución que esto representa, se diseñan y utilizan métricas de producto que permitan medir la complejidad de las bases de datos y de esta manera se estará midiendo la calidad del modelo lógico.

Una referencia completa de estas métricas se encuentra en Elsamary y Navathe [26].

En términos generales la calidad de un producto está dada por la cuantificación de las dimensiones de la calidad del mismo. Definir el marco de referencia de estas

dimensiones es el punto de partida para la medición, en este caso de la calidad de los datos.

Son importantes los trabajos que existen en esta materia, destacando el propuesto por Strong [27] donde se establece un conjunto de cuatro categorías de dimensiones de calidad, las cuales son descritos en la tabla 15.

Tabla 15. Dimensiones de la calidad de datos

Categoría de calidad de datos	Dimensiones de calidad de datos
Intrínsecas	Exactitud, objetividad, credibilidad, reputación
Accesibilidad	Relevancia, valor añadido, oportunidad, compleción, cantidad de datos
Contextual	Relevancia, valor añadido, oportunidad, complección, cantidad de datos
Representacional	Interpretación, facilidad de entendimiento, representación consistente

Dado que la calidad tiene componentes objetivos y subjetivos según Pipino [28], es necesario catalogar los requisitos de calidad de datos de los usuarios según las dimensiones de la calidad. Huang [24] propone considerar diferentes tipos de métricas correspondientes a esas componentes: subjetivas (basadas en el juicio de los usuarios de los datos), objetivas independientes de la aplicación (especificas para un dominio determinado).

De acuerdo al mismo tratamiento que se otorga a la producción de un producto para alcanzar las especificaciones y requisitos y por tanto la satisfacción del cliente, implementando sistemas de control de la calidad y de la mejora continua, los datos y la información vistos como producto deben de estar sometidos a un sistema de gestión de la calidad de los datos y por tanto de la Información.

Esto último tomando en consideración la definición de Información que hace Davenport [33] el cual establece:

Información = función (datos, contexto)

Tomando como base el estándar ISO 9001:2008, se diseñan y utilizan metodologías para la calidad y la mejora continua de los datos, de acuerdo al alcance de este trabajo referiremos la TQdM (Total Quality data Management) de Larry English [30].

TQdM atiende la mejora continua de dos categorías de procesos:

- Procesos de desarrollo de sistemas de información para definir información, desarrollando e implementando procesos de negocio, sistemas de información, y arquitectura de información y bases de datos
- Procesos de manufactura y negocios que crean, actualizan y borran datos, distribuyen o reparten información y recuperan o presentan información a los productores de información o a los trabajadores del conocimiento

La gestión de la calidad de la información consta de cinco procesos de medida y de mejora de la calidad de la información y un proceso que abarca a toda la organización para crear un entorno de calidad de información.

Los procesos que constituyen la metodología TQdM están descritos en la tabla 16.

Tabla 16. Metodología TQdM

Proceso	Pasos
1: Valoración de la Calidad de definición de datos y de la arquitectura de información	• Identificar las medidas de calidad de la definición de los datos • Identificar los grupos de información a valorar • Identificar a los implicados en la información • Valorar la calidad técnica de la definición de los datos • Valorar la calidad del diseño de la base de datos y de la Arquitectura de la información • Valorar la satisfacción de los clientes con la calidad de la definición de datos
2: Valoración de la calidad de la información	• Identificar los grupos de información que deben ser valorados • Establecer las medidas y los objetivos de la calidad de información • Identificar el valor de la información y la cadena de costos • Determinar los archivos o los procesos a valorar • Identificar las fuentes de validación de datos para valorar su exactitud • Extraer muestras aleatorias de datos • Medir la calidad de la información • Informar e interpretar adecuadamente la calidad de información
3: Medida de los costos de la no calidad	• Identificar las medidas de desarrollo del negocio • Calcular los costos de la información • Calcular los costos de la falta de calidad de información • Identificar segmentos de clientes

Proceso	Pasos
	• Calcular el valor del tiempo de vida del cliente • Calcular el valor de la información
4: Reingeniería y limpieza de datos	• Identificar las fuentes de datos • Extraer y analizar datos de las fuentes • Estandarizar datos • Corregir y completar los datos • Comparar y consolidar los datos • Analizar los tipos de defectos de datos • Transformar y mejorar los datos en los objetivos • Calcular las derivaciones y resumen de los datos • Auditar y controlar la extracción, transformación y carga de datos
5: Mejora de la calidad de los procesos de información	• Seleccionar los procesos para la mejora de la calidad de la información • Desarrollar un plan para la mejora de la calidad de la información • Implementar las mejoras de la calidad de la información • Comprobar el impacto de las mejoras de la calidad de la información • Actuar para estandarizar la mejora de la calidad de la información
6:Establecimiento del entorno de calidad de información	• Dirigir una valoración del grado de madurez de la gestión de la calidad de la información • Crear una visión, misión y objetivos • Identificar y enfatizar el rol del líder de calidad de información • Dirigir una valoración del grado de satisfacción de los clientes • Identificar otras transformaciones de negocio, iniciativas de mejora o recursos externos • Seleccionar un piloto, pequeño y manejable • Definir los problemas de negocio y medidas necesarias para resolverlos • Definir una cadena de valor y desarrollar un inventario de datos • Desarrollar una valoración de la calidad de la información • Calcular el valor del tiempo de vida del cliente • Cuantificar los costos de la no calidad en la información

Proceso	Pasos
6:Establecimiento del entorno de calidad de información	• Desarrollar lazos de confianza con los patrocinadores • Definir los roles y la plantilla de calidad • Definir principios, procesos y objetivos de calidad de datos • Analizar barreras sistemáticas • Ofrecer una formación formal en gestión de la calidad de información para directivos • Dirigir un proyecto de mejora de información • Establecer mecanismos regulares de comunicación, educación e implicación de los directivos • Mantener los procesos de mejora continua para la calidad de los datos

De acuerdo a lo anterior, la preparación de los datos para los procesos de personalización, se realiza en términos de la calidad que presentan las bases de datos de las entidades empresariales que participan en un programa de tarjetas inteligentes, siendo necesario en su caso aplicar un programa de limpieza o calidad de los datos existentes.

Para el caso de que no existan los datos con los que se han de personalizar las tarjetas, es recomendable que las aplicaciones de los diversos sistemas que los capturan contengan filtros y reglas de negocios que permitan desde el nacimiento de los datos que estos tengan niveles de calidad previamente definidos.

Medidas que contribuyen a mejorar la calidad de los datos, son el establecimiento de las normas y estándares que se deben de aplicar para la creación, uso y mantenimiento de catálogos comunes y diccionarios de las estructuras más comúnmente utilizadas, tales como nombres de calles, códigos postales, municipios, localidades e incluso nombres y apellidos, siendo la atomización de los nombres y las direcciones ejemplos de las normas referidas.

3.5 Sistema para la administración de llaves

3.5.1 Generalidades sobre la gestión de llaves

En el ámbito de las tarjetas inteligentes, una de sus fortalezas son los esquemas de seguridad que es aportada a partir de las técnicas y tecnología criptográfica con la que se cuenta en los microprocesadores y que de forma resumida se revisarón en el apartado 2.6.

De acuerdo con A. Gómez [39], existe una jerarquía de las llaves que se emplean en un sistema criptográfico, clasificándose en llaves maestras y llaves

subordinadas o como otros autores las denominan derivadas o de aplicación. Las llaves derivadas se utilizan para cifrar datos o aplicaciones dentro de las tarjetas inteligentes, mientras que las llaves maestras se utilizan para la protección de las llaves subordinadas, es decir del cifrado de las llaves derivadas.

Partiendo de Rankl [18], las llaves subordinadas se obtienen a partir de la aplicación de un número criptográfico, cuyos parámetros son un dato específico de la tarjeta y una llave maestra. De acuerdo al número especifico de la tarjeta, la llave subordinada obtenida es única dentro del programa de tarjetas.

Llave derivada = CIFRADO (llave maestra, número especifico de la tarjeta)

La figura 32 muestra este procedimiento.

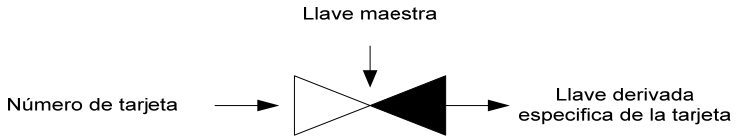


Figura 32. Método para derivar llaves simétricas

Una vez que son activadas las llaves, éstas podrán ser utilizadas para los distintos propósitos que se hayan definido, siendo recomendable emplearla solamente para una función. Diferentes llaves pueden ser utilizadas para las firmas de transmisión segura de datos, autenticación y cifrado de datos. Para cada tipo de llave debe haber una llave maestra separada, desde donde las llaves individuales pueden ser derivadas.

La primera medida relacionada con la validez y la destrucción de las llaves es la de definir un tiempo para su caducidad. Mientras mayor sea el periodo de utilización de una llave, mayor es la posibilidad de que ésta pueda ser comprometida.

Asimismo cuanto más se utilice una llave maestra mayor será el impacto de un ataque exitoso.

Otra clasificación que se le da a las llaves criptográficas es en atención al tiempo en que son utilizadas para una función específica, es decir se llaman llaves dinámicas, llaves temporales o llaves de sesión, a aquellas que se emplean para el cifrado de un único mensaje o para el cifrado de la información que ocurre durante la transmisión de la misma.

Para generar una llave dinámica, una de las dos partes que se comunica primero genera un número al azar o algún otro valor para su uso en una sesión específica,

y lo transmite a la otra parte. El curso posterior del proceso depende si los algoritmos criptográficos usados son simétricos o asimétricos.

Como lo detalla Wolfgang [17], las llaves dinámicas con algoritmos de cifrado simétrico, el número aleatorio generado por una de las dos partes se envía como texto plano a la otra parte. La tarjeta inteligente y la terminal entonces cifran este número usando una llave derivada. El resultado, como se muestra en la figura 33, es una llave que sólo es válida para una sesión en particular.

Llaves dinámicas = CIFRADO (llave derivada; número aleatorio)

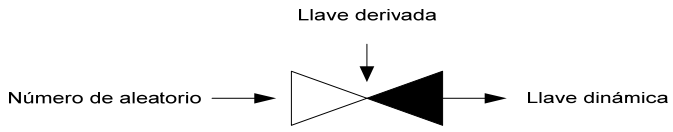


Figura 33. Generación de llaves dinámicas usando un número aleatorio y llaves derivadas

De acuerdo al procedimiento descrito, significa que cada vez que una llave dinámica se utiliza para una firma, el número aleatorio utilizado para generar la llave debe ser retenido para su uso en la verificación, lo que significa que debe ser almacenado.

Para el intercambio de llaves dinámicas utilizando un algoritmo criptográfico asimétrico, las figuras 34 y 35 muestran los procedimientos para la generación y, posteriormente el intercambio de una llave dinámica simétrica para mensajes cifrados.

El procedimiento de la figura 34 muestra el intercambio de llaves usando una combinación de algoritmos criptográficos simétricos y asimétricos. Una llave dinámica cifrada simétricamente es generada primero y luego intercambiada entre dos partes usando un algoritmo criptográfico asimétrico. La generación e intercambio del par de llaves por el algoritmo criptográfico asimétrico, el cual se toma separadamente no es mostrado.
Un algoritmo criptográfico asimétrico, como RSA, se utiliza para el intercambio de llaves. La ventaja fundamental de este proceso híbrido es que se puede realizar el cifrado real para grandes volúmenes de datos utilizando un cifrado con algoritmo simétrico que tiene un rendimiento significativamente mayor al de un algoritmo asimétrico.

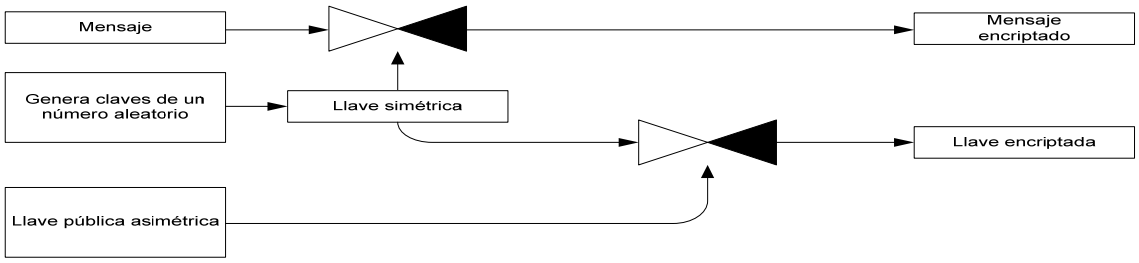


Figura 34. Procedimiento para el intercambio de llaves usando una combinación de algoritmos criptográficos simétricos y asimétricos

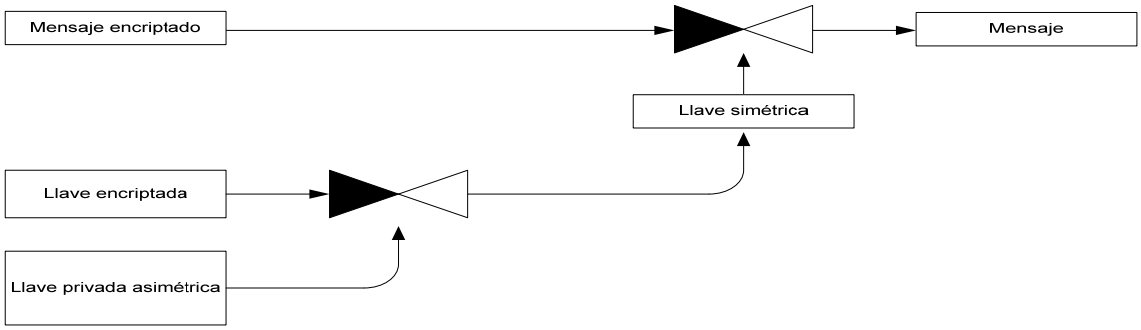


Figura 35. Procedimiento para el intercambio de llaves usando una combinación de algoritmos simétricos y asimétricos

Las llaves de manera general dentro de un sistema son utilizadas para diferentes fines. A fin de garantizar que una llave sólo se utilice para los fines para los que fue concebida, se debe vincular con un conjunto de atributos que definen la forma en que pueden ser utilizadas. El término llave para los propósitos de tarjetas inteligentes y de manera específica su relación con el SGTI, tiene un significado más amplio que el uso del término que se refiere solamente a su valor de cifrado.

Para evitar confusiones, aquí el término valor de llave se utiliza para describir el valor de cifrado, y el término perfil de llave se utiliza para describir un objeto que contiene el valor de la llave y un conjunto de atributos. Dependiendo del propósito de la llave, los atributos de contenido dentro de un perfil puede variar.

Como lo ejemplifica Global Platform [W7], el perfil1 y perfil2 de la llave no contienen un valor llave, esto normalmente sería el primer estado de un perfil de la llave, donde por ejemplo el uso se ha fijado. A partir de estos perfiles, los valores de la llave se pueden añadir básicamente utilizando el original como una plantilla, y con ello la creación de nuevos perfiles de la llave. Si el mismo valor llave se utiliza por dos entidades para fines diferentes, dos perfiles de llave serían necesarios, ya que debe contener atributos diferentes.

En el ejemplo se muestra la creación de los siguientes nuevos perfiles llave:

• Perfil1 llave creado con Atributos α, y perfil2 llave usando Atributos β
• Perfil3 llave basado en Perfil1 llave cuando llave está cargada, y perfil4 llave usando Atributos β

• Perfil5 basado en perfil1 llave cuando llave B está cargada, y perfil6 utilizando Atributos β • Perfil7a ….7c llave creados con atributos llave B dividido en 3 componentes, esta relación se muestra en la figura 36.

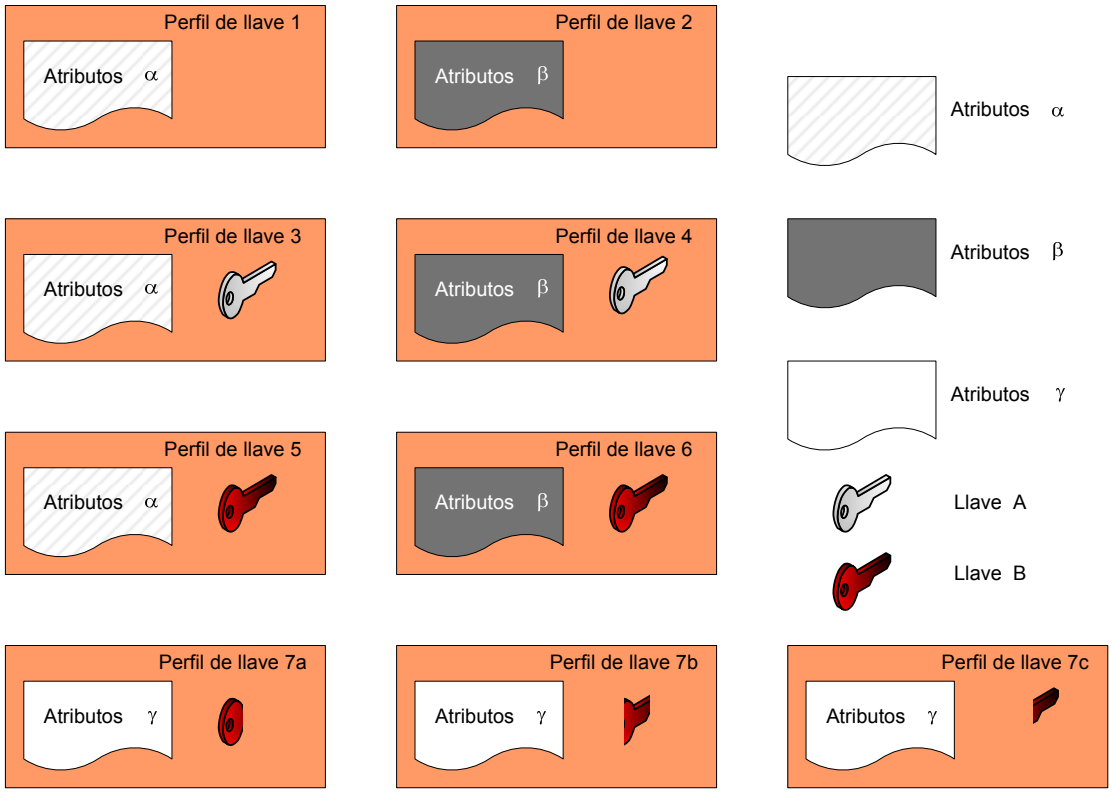


Figura 36. Relación entre valores de llaves, perfiles de llaves y atributos

3.5.2 Sistema para la gestión de llaves

De acuerdo a lo anterior, un sistema de gestión de llaves (SGLL) es un sistema, que de forma segura controla la generación, almacenamiento, distribución, uso y eliminación de las llaves criptográficas, valores y atributos. Un SGLL es parte de un sistema criptográfico que requiere de los valores de las llaves. Un sistema de gestión de llaves es típicamente un sistema basado en software haciendo uso de un cifrado basado en hardware del procesador para las operaciones de seguridad.

La gestión de llaves es una parte significativa de un Programa de tarjetas inteligentes. Es importante establecer cómo serán gestionadas las llaves,

especialmente si el Programa de tarjetas planea trabajar con más de una organización o entidad. El manejo de las llaves es el secreto del sistema. Si no son gestionadas adecuadamente, la integridad del sistema completo puede ser cuestionable y perder utilidad.

La gestión de llaves es una aplicación que es utilizada generalmente para mantener las llaves de cifrado. Una interfaz entre el SGTI y el sistema de gestión de llaves es necesaria y fundamental para importar las llaves al SGTI y que posteriormente puedan ser usadas de manera segura en las tarjetas.

De acuerdo al Government Smart Card Handbook, las principales funciones de la gestión de llaves son:

Función	Tareas
Registro	Verificación oficial Aplicación Registro y habilitación del chip
Generación de solicitudes de llaves y certificados	Solicita la carga de las aplicaciones y el borrado de los certificados Solicita los certificados a la autoridad certificadora
Almacenamiento de llaves y certificados	El HSM tiene requerimientos específicos

Tipo de llave	Función
Llave Global Platform	Son utilizadas para proteger la llave de la gestión de operaciones basadas en Java y regular las operaciones de la tarjeta
Contenedor de llaves	Control de acceso de lectura y escritura de datos
Llaves de transporte	Llaves temporales usadas para asegurar las tarjetas durante la transferencia del fabricante al emisor de la tarjeta
Llave de bloqueo del Pin	Habilita el reseteo del Pin

De manera general para cualquier sistema, de acuerdo al estándar ISO/IEC 11770 [W15] el ciclo de vida de una llave consta de cinco estados: generación, activación, desactivación, reactivación y destrucción.

De manera particular para la gestión de las llaves en tarjetas inteligentes, las normas y estándares que aplican son:

- ISO/IEC 7816 parte 8, comandos para la gestión de llaves
- ISO/IEC 11568 gestión de llaves, sector financiero
- ISO 10202 parte 7 gestión de llaves, tarjetas inteligentes
- ISO/IEC 15946 técnicas criptográficas basadas en curvas elípticas
- EMV parte 2 gestión de llaves
- ANSI X9.69, gestión de llaves

De acuerdo a la especificación de Global Platform [W7] se concibe un sistema de gestión de llaves como:

- Una base de datos para el almacenamiento de los valores y atributos de las llaves
- Un generador de servicios que necesiten los valores de las llaves, generalmente en forma de una API
- Un módulo de hardware seguro (HSM por sus siglas en inglés) para garantizar la secrecía, la integridad de los valores y atributos, y también el de proporcionar el recurso para la generación del valor de la llave a partir del cálculo matemático intensivo

3.5.2.1 Requisitos del sistema de gestión de llaves

Global Platform establece los siguientes requisitos generales de un SGLL (KMS por sus siglas en inglés)

a) De acuerdo al estándar ISO/IEC 11770, el SGLL deberá de ser capaz de mantener los perfiles de la llave durante todo el ciclo de vida de los perfiles, desde la definición, la generación, el almacenamiento, intercambio, utilización, vencimiento y cancelación

b) El SGLL prestará servicios a los sistemas asociados que tengan la necesidad del uso de un perfil específico de llave. Estos servicios proporcionan un mecanismo para que los usuarios del SGLL generen intercambio y recuperación de llaves

c) El SGLL tendrá funciones de secrecía o críticas (como la generación o desempacar / empacar los valores de las llaves) las realizará dentro de un módulo de hardware seguro o componente de seguridad equivalente (HSM)

d) El SGLL deberá de ser capaz de recuperar todos los perfiles de llave dentro del SGLL, en caso de falla en el mismo sistema SGLL o en el HSM utilizado

Las siguientes son especificaciones que debe de cumplir un SGLL

- Requisitos para el acceso y auditoría

- Requerimientos de soporte a los algoritmos criptográficos y de sus diferentes modos
- Requisitos para los perfiles de las llaves
- Requisitos para la generación de las claves
- Algoritmo TDEA
- Algoritmo RSA
- Requisitos para la revocación de llave
- Requisitos para almacenar llaves
- Requisitos para intercambio de llaves
- Intercambio de perfiles de llave.
- Intercambio de llaves TDEA.
- Intercambio de llaves RSA
- Requisitos para importar y exportar llaves
- Requisitos para la separación de llave
- Requisitos para la comprobación de fecha
- Requisitos para la caducidad y eliminación

Los requisitos que recomienda Global Platform para un módulo de hardware seguro son los siguientes:

3.5.2.2 Requisitos del módulo de hardware seguro

a)
- Generación de valores de las llaves
- Intercambio de los valores de las llaves
- Separación de los perfiles de las llaves (división lógica de atributos de las llaves)
- Exportación e importación de llaves
- Almacenamiento seguro de los valores de las llaves
- Las pruebas de generación de números aleatorios se llevarán a cabo periódicamente para comprobar que sigue funcionando correctamente de acuerdo a la norma FIPS 140-2[R8]

b) Los servicios ofrecidos por el HSM, además de los requisitos establecidos en este documento, no se permiten eludir los requisitos del HSM Global Platform SGLL, por ejemplo, el SGLL requiere la separación del perfil, el HSM no debe ofrecer servicios adicionales o tradicionales que permitan la separación de la llave para ser anulada.

c) El HSM deberá estar certificado en un nivel correspondiente al menos en FIPS 140-2 nivel 3.

3.6 Interfaces del SGTI con otros sistemas de información

De acuerdo con Taro y Wada [R21], en la figura 37, se ilustra un ambiente de operación multiaplicaciones, donde se requieren diversos servicios proporcionados por varias entidades empresariales, los cuales son soportados por diferentes sistemas de información.

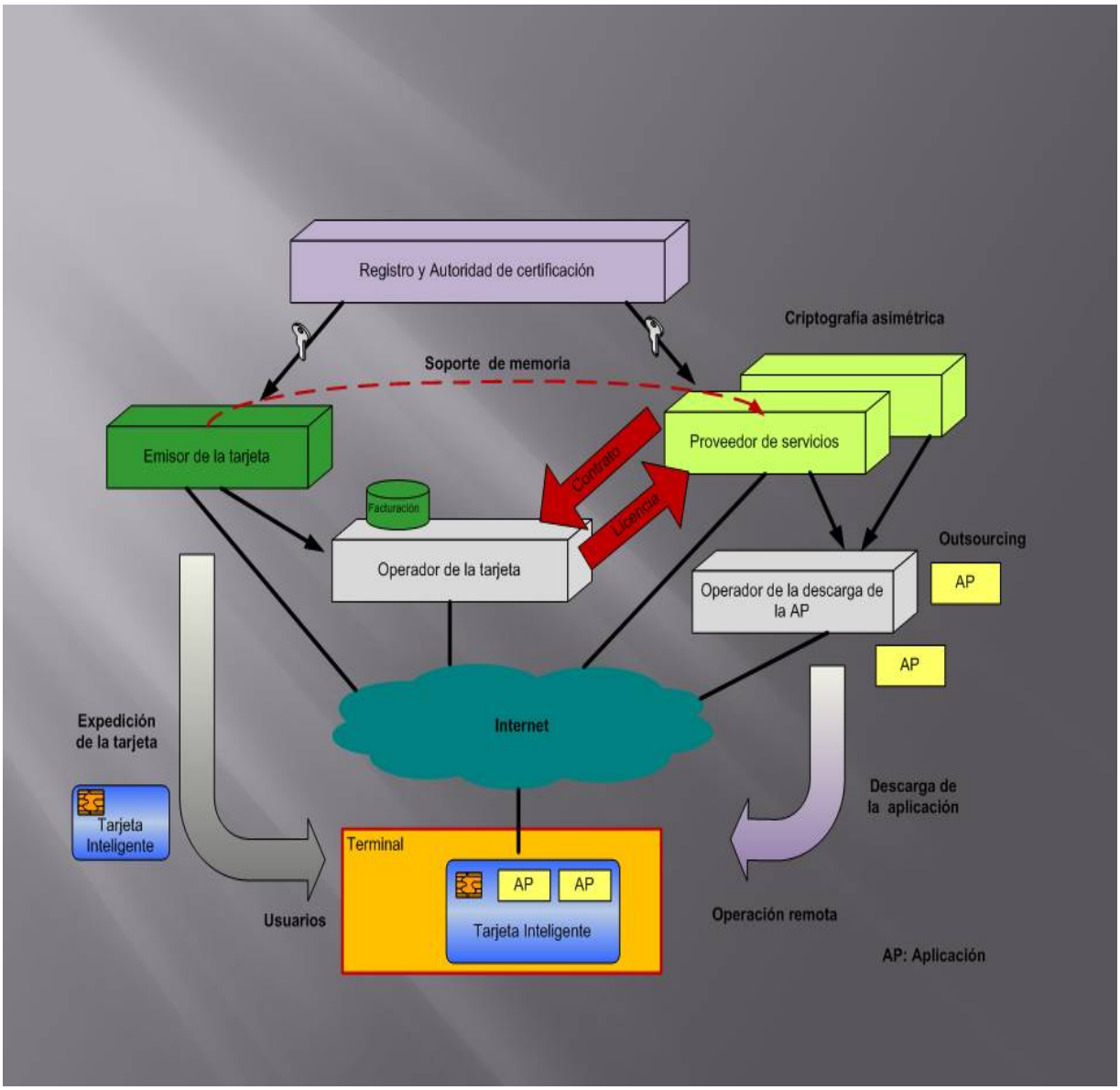


Figura 37. Servicios soportados en la gestión de una tarjeta inteligente por diferentes sistemas de información

En un Programa de tarjetas inteligentes, el SGTI interacciona con diversos sistemas de información, de acuerdo a las diferentes funcionalidades que se requieren durante su ciclo de vida útil, así como procesos de uso y explotación de

la información que se genera durante el, los principales sistemas de información se describen en la tabla 17, en la tabla 18 se presenta la intersección de los sistemas que tienen interfaces entre si.

Tabla 17. Descripción de los sistemas de información que participan en un ambiente SGTI

Sistemas de información en un Programa de tarjetas inteligentes	Descripción
SGTI	Gestión de tarjetas inteligentes
Sistema para la gestión de llaves (SGLL)	Gestiona el ciclo de vida de las llaves de las tarjetas inteligentes
Sistema colector de transacciones electrónicas (SCTE)	Integra las transacciones electrónicas derivadas de la operación de las tarjetas inteligentes
Sistema de autorización (SA)	Recibe y atiende las peticiones de autorización de transaciones electronicas
Sistema de atención a clientes (SATC)	Recibe y atiende los reportes de eventos ocurridos con las tarjetas inteligentes
Sistema de relaciones con los clientes (SRC)	Registra, consolida, procesa y analiza, las operaciones realizadas por tipo de transacion de los clientes
Sistema de enrolamiento (SE)	Captura y procesa los datos de los titulares de las tarjetas
Sistema de emisión (SEM)	Personaliza gráfica y eléctricamente las tarjetas
Sistema de planeación y control de la producción (SPCP)	Gestiona y controla la producción de las tarjetas de acuerdo a los requerimientos de los emisores
Sistemas de operadores (SP)	Administra la operación de los programas de las tarjetas
Sistemas de proveedores de servicios (SPS)	Administra los diversos bienes y servicios que requieren los emisores, habilitadores, cargadores
Sistemas de autoridades certificadoras (SAC)	Administra las peticiones de certificados requeridos por la industria de tarjetas

Tabla 18. Intersección entre los sistemas de información que participan en un ambiente SGTI, que tienen interfaces entre si

	SGTI	SGLL	SCTE	SA	SATC	SRC	SE	SEM	SPCP	SP	SPS	SAC
SGTI	X	X	X		X	X		X	X	X	X	
SGLL	X	X						X			X	X

	SGTI	SGLL	SCTE	SA	SATC	SRC	SE	SEM	SPCP	SP	SPS	SAC
SCTE	X		X							X	X	
SA				X	X			X		X	X	X
SATC	X			X	X	X				X		
SRC	X				X		X				X	
SE						X		X	X	X	X	X
SEM	X	X		X				X	X	X	X	X
SPCP	X						X	X	X	X		
SP	X		X	X	X		X	X	X	X	X	
SPS	X	X	X	X		X	X	X		X	X	
SAC		X		X			X	X				X

Las entradas y salidas de los sistemas de información en el ambiente de operación SGTI, se relacionan en la tabla 19.

Tabla 19. Entradas y salidas de los sistemas relacionados con el SGTI

Sistema	Entradas	Salidas
Sistema de gestión de tarjetas inteligentes SGTI	Requerimientos funcionales	Portafolio de productos
	Especificaciones según normas y estándares	Portafolio de productos
	Perfil de plataforma de tarjetas	Tarjetas inteligentes personalizadas gráfica y eléctricamente
	Perfil de tarjetas	Especificaciones de tarjetas
	Perfil de chips	Especificaciones de chips
	Perfíl de sistemas operativos	Especificaciones de sistemas operativos
	Perfil de llaves	Especificaciones de llaves
	Solicitud de llaves	Llaves según solicitud
	Estado inicial del ciclo de vida de la tarjeta	Estados del ciclo de vida de la tarjeta
	Perfil de aplicaciones	Especificaciones de aplicaciones
	Solicitudes de	Aplicaciones cargadas en

Sistema	Entradas	Salidas
	aplicaciones según perfil	las tarjetas
	Estado inicial del ciclo de vida de las aplicaciones	Estado final del ciclo de vida de las aplicaciones
	Reportes de cargas/descargas de aplicaciones	Detalle de reportes de procesos de carga/descarga de aplicaciones
Sistema gestión de llaves (SGLL)	Perfil de llaves	Llaves de acuerdo a un perfil
	Solicitud de llaves	Llaves según solicitud
Sistema colector de transacciones electrónicas (SCTE)	Perfil de tarjetas	
	Perfil de aplicaciones	
	Tarjetas emitidas	
	Aplicaciones cargadas	
	Perfil de titulares de tarjetas	
	Directorio de emisores	
	Perfil de proveedores de servicios	
	Red de TPV	
	Solicitudes de transacciones	Transacciones electrónicas
	Listas calientes	Listas calientes aplicadas
		Reportes de transacciones
	Perfil de terminales	
	Catalogo de terminales	
	Ubicación de terminales	
Sistema de autorización (SA)	Catálogo de programas	
	Catálogo de operadores	
	Catalogo de emisores	
	Tipo de autorización	Respuesta a la solicitud
	Número de solicitud	Número de autorización
	Titulares de tarjetas	
Sistema de atención a clientes (SATC)	Catálogo de emisores	
	Portafolio de productos por emisor	
	Catalogo de dueños de tarjeta	
	Catálogo proveedores de servicio	
	Solicitudes de información	Atención a solicitudes

Sistema	Entradas	Salidas
	Reportes sobre tarjetas	Atención a reportes
Sistema de relaciones con clientes (SRC)	Perfil de tarjetas	
	Catálogo de emisores	
	Catálogo de proveedores de servicios	
	Catálogo de productos	
	Transacciones electrónicas por titular de tarjeta	Estadística del comportamiento del titular de la tarjeta
	Transacciones electrónicas por emisor	Estadística del comportamiento de las tarjetas por emisor
	Transacciones electrónicas por proveedor de servicios	Estadística del comportamiento de las tarjetas por proveedor de servicios
Sistema de enrolamiento (SE)	Perfil de titulares de tarjeta	
	Perfil de tarjeta	
	Estructura de datos a capturar	Datos capturados
	Requerimientos de datos físicos a capturar	Datos físicos capturados
Sistema de emisión (SEM)	Catálogo de programas	
	Catálogo de perfiles tarjetas	
	Catálogo de perfiles aplicaciones	
	Titulares de tarjetas	Tarjetas emitidas
	Catálogo de operadores	
Sistema de planeación y control de la producción (SPCP)	Catálogo de materiales Catálogo de mano de obra Programas de producción Catálogo de equipo y herramienta Catálogo de la explosión de materiales	Catálogo de producto terminado
Sistema de operadores (SP)	Catálogo de programas de tarjetas inteligentes Catálogos de perfiles de tarjetas, aplicaciones, socios de negocios,	Transacciones de la operación de los programas

Sistema	Entradas	Salidas
	emisores	
Sistemas de proveedores de servicios (SPS)	Catálogo de provedores Catálogo de servicios que proporcionan	Transacciones de la operación de los servicios que se proporcionan
Sistemas de autoridades certificadoras (SAC)	Catálogo de servicios	Transacciones de la interacción con emisores, proveedores de aplicaciones

Las figuras 38 y 39 muestran un ejemplo de interacción entre las tarjetas inteligentes, el SGTI, sistemas de emisores y de otras entidades empresariales, como puede ser un operador de programa de lealtad.

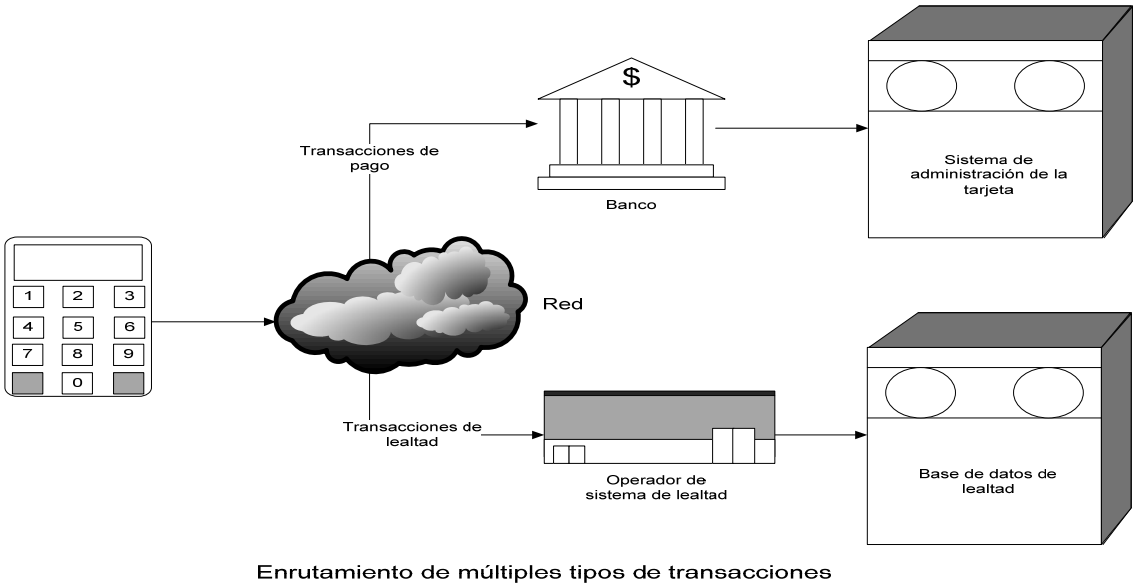


Figura 38. Operación de una tarjeta inteligente gestionada por el SGTI, con interfaces de los sistemas del emisor y del operador del programa de lealtad

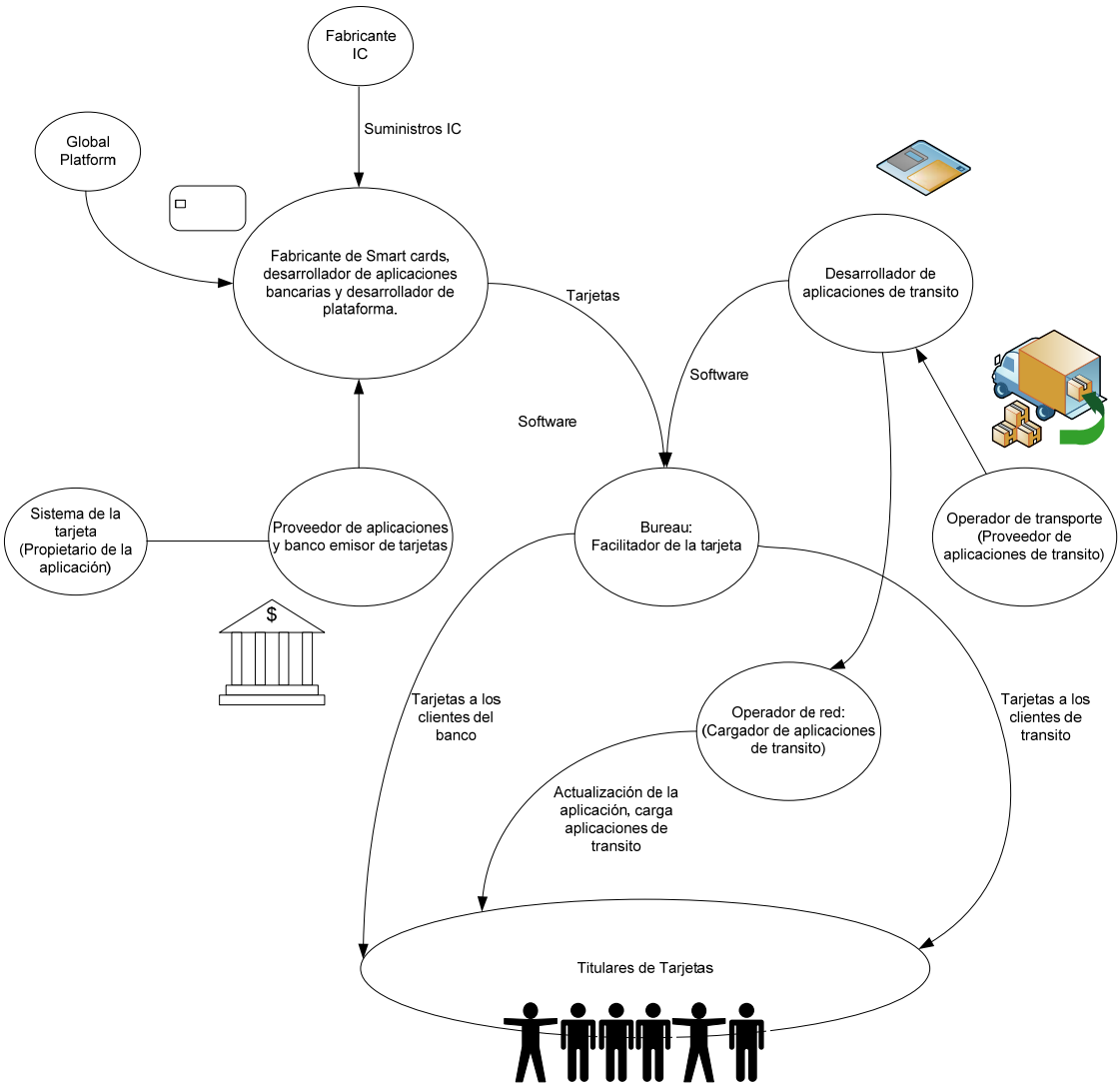


Figura 39. Interfaces entre sistemas de información de entidades empresariales involucradas con el SGTI

3.7 Infraestructura requerida

3.7.1 Infraestructura asociada a los sistemas relacionados con el SGTI

De acuerdo a los requerimientos el ambiente del SGTI, puede operar de manera centralizada o descentralizada, y dependiendo del alcance del Programa de tarjetas inteligentes, se determina la configuración de operación entre las entidades empresariales que participan y la topología de la infraestructura y de los sistemas de información de acuerdo a la funcionalidad y roles de cada uno de ellos.

De esta forma existen diversas alternativas de configuraciones para llevar a cabo la operación.

La tabla 20 enuncia los principales sistemas de información que pueden interactuar en un programa de tarjetas inteligentes, la forma típica de operación y la infraestructura tecnológica que se requiere.

Tabla 20. Infraestructura de los sistemas relacionados con el SGTI

Sistema	Tipo de Operación	Infraestructura
SGTI	Centralizada	Servidor de aplicaciones Servidor de base de datos Sistema de Gestión de Base de Datos Red de comunicaciones Sistema de seguridad perimetral Equipos de personalización
Sistema de enrolamiento (SE)	Descentralizada	Equipo de captura de datos físicos y alfanuméricos Estación de captura de datos biométricos (huella digital, iris, reconocimiento de firma, geometría del rostro, retina) Impresoras Escáner de documentos Red de comunicaciones Sistema de seguridad
Sistema de emisión (Subsistema de personalización electrica) (SEM)	Centralizada	Equipamiento de personalización en planta
Sistema de emisión (Subsistema de personalización gráfica) (SEM)	Centralizada/Descentralizada	Equipo de captura de datos físicos y alfanuméricos
Sistema gestion de llaves (SGLL)	Centralizada	Servidor de llaves Estación de generación de llaves HSM
		Lectores de tarjetas para contactos Lectores de tarjetas sin contactos PC con lectores Terminales punto de venta

Sistema	Tipo de Operación	Infraestructura
Sistema colector de transacciones electrónicas (SCTE)	Descentralizada	Equipos ATM Maquinas vending Equipos de control de acceso Pads para Pin Equipos de comunicaciones y red de switcheo a las entidades empresariales que autorizan movimientos
Sistema de relaciones con cliente (SRC)	Centralizada	Sistema de CRM Call Center Red de comunicaciones Computadoras Personales
Sistema de proveedores de servicios (SPS)	Descentralizada	Red de telecomunicaciones
Sistema de planeación y control de la producción (SPCP)	Centralizada	Servidores de datos
Sistema de autoridades certificadoras (SAC)	Centralizada	Servidores de datos
Sistema de autorización (SA)	Centralizada	Servidores de datos

La configuración y capacidades de la infraestructura se obtienen a partir de la administración de la demanda, la administración de la seguridad de la información, el plan de continuidad del negocio, temas que abordaremos en el apartado de la arquitectura tecnológica.

3.7.2 Administración de la terminal

Considerando los requerimientos de seguridad y compatibilidad necesarios para la correcta operación del ambiente de tarjetas inteligentes revisaremos las características de las terminales de lectura de las tarjetas.

De acuerdo con Hendry [19], las terminales de lectura de tarjetas inteligentes son mucho más complejas en los últimos años. En la década de 1990 se trasladaron

de la lógica fija a una con base en firmware, no obstante, el software en sí era relativamente simple y eran pocos los parámetros variables. Con la llegada de las tarjetas con chip, ahora son más complejas. Las terminales que soportan estas tarjetas tienen memoria desde 256 KB hasta 8 MB, la mayoría de programas de soporte a múltiples aplicaciones deben de incluir funciones de cifrado para garantizar la seguridad de la propia terminal y los datos que se intercambian entre la terminal y el servidor anfitrión.

Las terminales ocultan esta complejidad mediante un software que hace que las nuevas funciones sean transparentes para el usuario, pero ahora hay una necesidad de gestionar parámetros adicionales de software.

Para las terminales de banda magnética, el fabricante casi siempre produce el software. Probablemente fue escrito en un lenguaje de bajo nivel y consistía principalmente en controladores para los diferentes dispositivos de la terminal y un flujo de lógica simple, como las terminales se utilizan en nuevos mercados, las instrucciones podrían ser fácilmente adaptadas para diferentes idiomas y entornos de venta.

El software de terminales de tarjetas de chip es mucho más especializado, y cada nueva aplicación de una nueva tarjeta requiere de un nuevo software para terminal. Hay, por tanto, un movimiento hacia la utilización de casas de software especializado para crear el software de aplicaciones para las terminales, estas prefieren trabajar en lenguajes de alto nivel a fin de que puedan vender sus aplicaciones a muchos clientes, incluidos los vendedores de terminales.

Esto, a su vez, conduce a una demanda de estructuras de terminales e interfaces normalizados, lo que condujo a la creación de la STIP (Small Terminal Interoperabily Interface).

Los cambios importantes del software de terminales eran raros y no eran de cifrado de llaves. Por lo tanto, era factible mantener estas terminales con métodos manuales (visitas de ingeniero de soporte o soporte en línea).

El software para terminales de tarjetas con chip, evoluciona continuamente, en la medida que se desarrollan nuevos productos, nuevas características se introducen en los productos actuales. Cuanto más complejo es el software, puede tener más errores, o se puede encontrar que los usuarios prefieren la redacción ligeramente diferente de un sistema.

Cuando se utiliza criptografía para proteger los datos o las transacciones, las terminales deben almacenar llaves para cada aplicación o emisor de la tarjeta, a menudo de varias longitudes y versiones. Si una llave caduca o puede haber estado en peligro, entonces rápidamente se debe quitar de las terminales y se reemplaza con una llave actualizada. Debido al limitado tiempo disponible para

realizar estos cambios, y la necesidad de proporcionar una pista de auditoría y el proceso de verificación, es esencial que se realicen por vía electrónica. Estas nuevas terminales son computadores de gran alcance, que si en ellas solamente se ejecuta una aplicación, están subutilizadas la mayor parte del tiempo. Las terminales de sistemas de múltiples aplicaciones deben permitir realizar muchas más funciones, y muchas veces mejorar la economía de la utilización de la terminal. Las terminales deben ser programadas para hacer uso de estas funciones adicionales, las nuevas funciones y formas de añadir valor puede aparecer con bastante frecuencia, y para aprovechar de estas oportunidades es importante que los estados de todas las terminales puedan ser actualizadas rápidamente. En este contexto, los propietarios y operadores de terminales de medianas cantidades (de unos pocos cientos de terminales hacia arriba) saben que el anterior método manual de actualización de las terminales es insuficiente, un sistema de gestión de terminales (TMS, por sus siglas en inglés) es necesario.

Las principales funciones de un TMS, ver figura 40, son las siguientes:

- Mantener un registro de todos los bienes propietarios de una terminal, incluyendo el hardware y versiones de software, las versiones de llave pública y las instalaciones habilitadas
- Gestionar la descarga eficiente de las aplicaciones, los parámetros y llaves para todas las terminales
- Una vez que una nueva aplicación, actualización de la aplicación o el cambio de parámetro está descargado, se provoca un cambio en el nuevo software o se debe de asesorar al usuario para que realice una acción para efectuar el cambio
- En el caso de las descargas de gran tamaño, comprimir o dividir la descarga, para reducir al mínimo el tiempo necesario, y para manejar los errores que surjan durante la descarga
- Responder a las solicitudes de la terminal para las descargas (por ejemplo, en la instalación inicial o después de una falla)
- Periódicamente subir (por cobrar) el seguimiento y diagnóstico de los archivos desde las terminales en la terminal que los genera

Muchas terminales modernas están programadas en la plataforma de lenguajes independientes, como Java C++. Con estas terminales, cada vez es posible desarrollar aplicaciones que se ejecutan en varios tipos de terminales diferentes. Algunas de estas aplicaciones pueden ser para las funciones especializadas o servicios específicos, y pueden ser desarrolladas por compañías de software que no sea el proveedor de terminales. En estos casos el TMS también debe manejar los certificados de la aplicación y la aplicación de la carga de proceso.

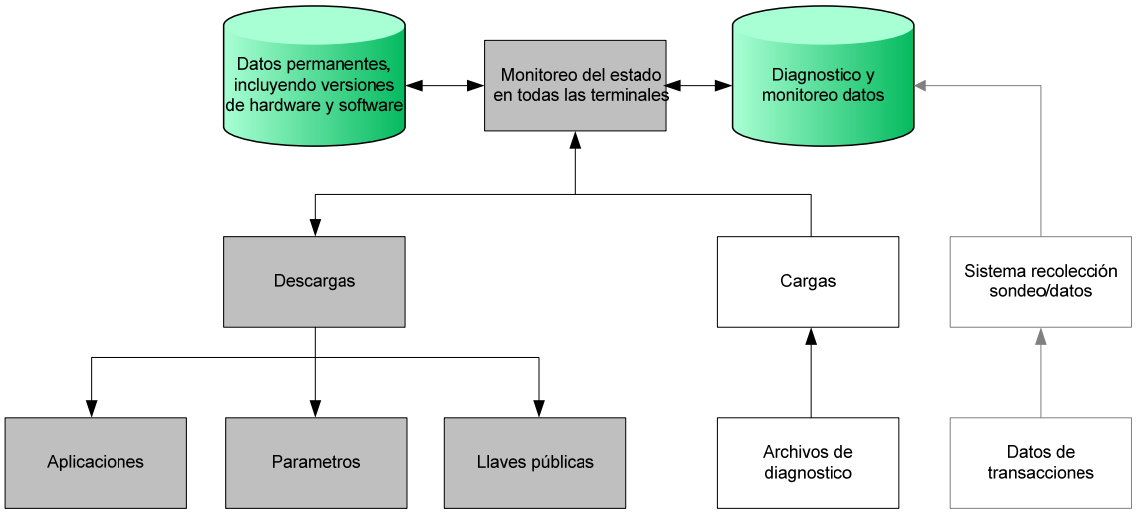


Figura 40. Principales funciones de un TMS

3.8 Estándares relacionados con el SGTI

En este apartado se resumen las normas y estándares que aplican a un SGTI, al sistema administrador de llaves y al módulo de hardware seguro.
También se incluyen los estándares, buenas prácticas y diferentes marcos de referencia para el despliegue de la especificación que aplican a este trabajo.

Diccionario 7. Estándares que aplican al SGTI

Estándar	Descripción/Referencia	Aplica a:
Global Platform	Global Platform Card Specification V2.1 Global Platform Key Management System V1.0 SCMS Functional Requirements V4.0	SGTI
ISO/IEC 10202-1	Ciclo de vida de tarjetas inteligentes Apartado 2.8.3	SGTI Procesos de tarjetas inteligentes
ISO/IEC 14443	Tarjetas de identificación, tarjetas de circuitos integrados sin contactos, tarjetas de proximidad Apartado 2.8.1	Perfiles de tarjetas inteligentes
ISO/IEC 11770	Tecnología de la información, técnicas de seguridad, administración de llaves Apartado 2.8.6	SGLL Tarjetas inteligentes
ISO 24727	Compatibilidad e interoperabilidad entre aplicaciones de diferentes tarjetas y sistemas operativos	SGTI Tarjetas inteligentes

Estándar	Descripción/Referencia	Aplica a:
	Apartado 2.8.4	
ISO/IEC 7816	Tarjetas de identificación, tarjetas de circuitos integrados con contactos Apartado 2.8.1	Perfiles de Tarjetas inteligentes
EMV 2000 Libro 1 al 4	Especificación de tarjetas de circuitos integrados para sistemas de pagos Apartado 2.8.4	Especificación para aplicaciones bancarias SGLL
Comandos APDU	Comandos APDU y los ciclos de vida	SGTI Tarjetas inteligentes Procesos de ciclo de vida
FIPS 46-3: 1999	Describe los algoritmos DES y triple DES	Tarjetas inteligentes HSM
FIPS 81: 1980	Modos de operación de DES	Tarjetas inteligentes SGLL HSM
FIPS 140-2: 2001	Requerimientos de seguridad para módulos criptográficos	Tarjetas inteligentes SGLL HSM
FIPS 197: 2001	Estándar de cifrado avanzado (AES) Describe el algoritmo AES	Tarjetas inteligentes SGLL HSM
IEEE 1363: 2000	Estándar cifrado de datos (DES)	Tarjetas inteligentes SGLL,HSM
GSC-IS Versión 2.1	Gobierno de interoperabilidad para tarjetas inteligentes elaborado por el NIST del Gobierno de Los Estados Unidos	SGTI Aplicaciones de tarjetas inteligentes
TOGAF	Arquitectura empresarial de información	Marco de referencia de la arquitectura del SGTI
ISO/IEC 20000:2005	Gestión de calidad de procesos de tecnología de la información	Gestión y soporte de servicios del SGTI
ISO 9001:2008	Gestión de la calidad	Gestión de la calidad de los procesos plataforma de gobierno del SGTI
ITIL	Gestión y soporte de servicios de TI	Implementación y gobierno del SGTI

Estándar	Descripción/Referencia	Aplica a:
PMI	Administración de proyectos	Plan de migración e implementación del SGTI
ISO/IEC 27001	Gestión de la Seguridad de la Información	Plataforma de gobierno del SGTI
CMMi	Nivel de madurez organizacional	Plataforma del gobierno del SGTI
Cadena de valor	Modelo de cadena de valor	Modelado de la arquitectura de negocios

Capítulo 4

Implementación del SGTI

4.1 Propuesta de metodología para la implementación de un SGTI

I) Los principales componentes y características de una tarjeta inteligente que hemos revisado son:

- Microprocesadores y su hardware en general
- Especificaciones eléctricas de los microprocesadores
- Sistemas operativos
- Fundamentos de la seguridad basada en algoritmos criptográficos,
- Estándares y normas
- Ciclos de vida de tarjetas y aplicaciones y,
- Su arquitectura

II) Los conceptos y referentes que están directamente asociados con el SGTI:

- Visión general de sus funcionalidades
- Condiciones para el proceso de preparación de datos para la personalización de las tarjetas
- Procesos asociados a la gestión de llaves criptográficas
- Interrelación e interfaces que tiene con otros sistemas de información
- Visión general de la infraestructura necesaria para que opere y,
- Estándares de aplicación

A partir de este punto vamos a asociar e integrar los temas referidos para conformar las especificaciones del sistema de gestión para tarjetas inteligentes.

Como se estableció en el apartado de sistemas de información de este trabajo, la integración se realizará a partir del marco de referencia de TOGAF [W10].

TOGAF es un marco de referencia de arquitectura empresarial de información (AEI), cuyo modelo está integrado por cuatro capas arquitectónicas:

- Negocios,
- Datos,
- Aplicaciones,
- Tecnológica

El método de desarrollo de la AEI señala que las fases son iterativas, iniciando con líneas base y avanzando en versiones que se construyen a partir de la retroalimentación del ciclo anterior, ver figura 41.

La característica del método es su orientación a procesos, dejando al arquitecto los métodos para su construcción.

Cada una de las fases se describe en la tabla 21.

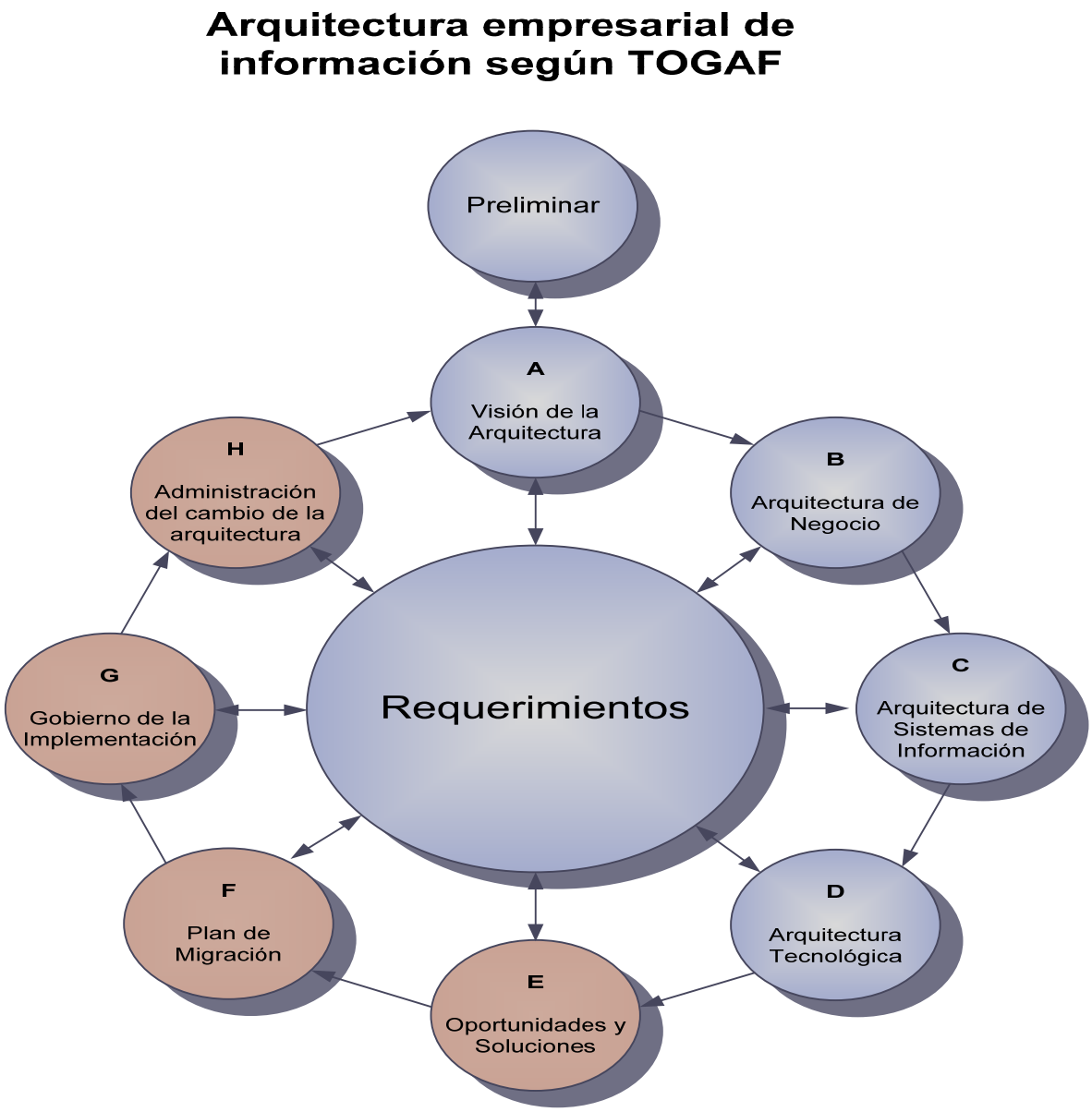


Figura 41. Ciclo de vida del marco de referencia de TOGAF

Tabla 21 Descripción de las fases de la AEI, según TOGAF

Fase	Descripción
Preliminar	Identificación del medio ambiente de la organización, así como de los principales involucrados y herramientas
Visión de	Desplegar el alcance, identificar los componentes de la arquitectura, visualizar los impactos del desarrollo de la

arquitectura	arquitectura
Arquitectura de negocios	Estructura formal del modelo de negocios, conocer sus interrelaciones, productos y procesos
Arquitectura de información	Modelo de la organización a partir de las arquitectura de aplicaciones, la cual permitirá automatizar los procesos de la organización y la arquitectura de datos, la cual permitirá reflejar en estructuras de datos, los resultados de la operación de la organización
Arquitectura tecnológica	Estructura formada por varias capas de tecnología y sistemas de gestión de la calidad y seguridad, para ser el soporte de las arquitecturas de aplicaciones y datos
Oportunidades y soluciones	Fase en la cual se identifican las lagunas o inconsistencias entre las arquitecturas previas, para su neutralización y mejora
Plan de migración	Conjunto de actividades programadas, con el fin de acceder a la nueva arquitectura
Gobierno de la implementación	Mecanismo mediante el cual se establecen las reglas, roles y procedimientos para llevar a cabo la migración hacia la nueva arquitectura
Administración del cambio de la arquitectura	Procesos mediante los cuales se administra la operación de la nueva arquitectura

En este trabajo, la Fase H se desarrolla en el apartado de Gobierno del SGTI.

En consecuencia la metodología que se propone para la implementación del SGTI es la siguiente:

1) Identificar para cada fase, a que etapa del proyecto corresponde. conceptualización, modelado e implementación

2) Por fase identificar los objetivos y entregables

3) Determinar las herramientas, métodos, técnicas o mejores prácticas que se encuentren en el estado del arte que serán empleadas en el desarrollo de las fases.

4) A partir de las herramientas seleccionadas obtener los entregables de la fase que corresponda

5) Revisar los entregables y validar su compatibilidad con respecto a fases anteriores

6) Actividades de retroalimentación del desarrollo de los entregables

4.2 Desarrollo de la metodología propuesta

4.2.1 Identificar para cada fase a que etapa corresponde, conceptualización, modelado, implementación

Etapa	Fases que lo comprenden
Conceptualización	Preliminar, A
Modelado	B,C,D
Implementación	E,F y G

4.2.2 Por fase identificar los objetivos y entregables

Tabla 22. Fase: Preliminar

Objetivos
• Revisar el contexto de la organización para la realización de arquitectura empresarial • Identificar las partes interesadas, patrocinador (es) y otras partes interesadas importantes afectadas por la dirección de negocio para crear una arquitectura empresarial • Determinar sus necesidades y prioridades con la empresa, sus relaciones con la empresa • Asegurar que todos los que estarán involucrados están comprometidos con el éxito del proceso arquitectónico • Habilitar al patrocinador de la arquitectura, para crear los requisitos para trabajar a través de las áreas de negocio afectadas • Identificar el alcance de los elementos de las organizaciones empresariales afectadas por la dirección de negocios y definir las limitaciones y supuestos • Definir el marco y metodologías detalladas que se van a utilizar para desarrollar la arquitecturas de la empresa • Confirmar un marco de gobierno y de apoyo que proporcionarán los recursos para el gobierno • Seleccionar y aplicar herramientas de apoyo y otras infraestrcuturas destinadas a apoyar la actividad de la arquitectura • Definir los principios de arquitectura que formarán parte de las limitaciones en cualquier arquitectura de trabajo

Entregables
Para el caso que nos ocupa, referiremos a una empresa, cuyo foco de negocio es la producción de tarjetas inteligentes, con atención de mercados internacionales, proveedores locales e internacionales. En este contexto, las entidades empresariales que requieren esta herramienta

Entregables
pueden ser, los fabricantes de tarjetas, los emisores o los dueños de las aplicaciones. Una por si sola de estas entidades empresariales no genera todos los procesos que ocurren durante el ciclo de vida de las tarjetas inteligentes y aplicaciones por lo que es necesario para cada caso en particular conocer las interfaces de producción entre ellos y trasladarlas a las interfaces de los sistemas de información propiedad de cada entidad. Otro aspecto a considerar, en el caso de que una sola entidad administre el SGTI, es el ambiente de la operación, que puede ser centralizado o descentralizado Para los efectos de este trabajo, supondremos que una sola entidad administra el SGTI, dando servicio a las otras entidades empresariales, según su área de competencia. En este sentido el alcance del SGTI serán los procesos productivos de preemisión, emisión y postemisión.

Tabla 23. Fase A: Visión de Arquitectura

Objetivos
• Asegurar que la evolución del ciclo de desarrollo de la arquitectura, tiene el reconocimiento y apoyo de la administración corporativa y el soporte necesario de la gerencia • Validar los principios del negocio, metas de negocio y conducción estratégica de negocios de la organización • Definir el alcance, identificar y priorizar los componentes de la arquitectura • Definir las entidades empresariales relevantes involucradas y sus objetivos • Definir los requerimientos claves de negocios, a ser direccionados en los esfuerzos de la arquitectura y las condiciones para lograrlo • Articular un visión arquitectónica, que demuestre una respuesta a los requerimientos y condiciones • Asegurar los procedimientos formalmente aprobados • Entender los impactos sobre/y de otros esfuerzos en paralelo del ciclo de desarrollo de la arquitectura

Entregables
• Misión • Visión • Valores • Política de Calidad • Política de Seguridad

Entregables
• Objetivos generales (de negocio) • Objetivos particulares (de negocio) • Estrategias • Procesos • Proyectos • Metas • Organigrama • Manuales de organización y procedimientos • Normas internas y contractuales • Plan de negocios

Tabla 24. Fase B: Arquitectura de negocios

Objetivos
• Describir una Línea base de Arquitectura de negocios • Desarrollar la salida de la Arquitectura de negocios, describiendo los productos y/o servicios estratégicos, y aspectos organizacionales, funcionales, de procesos, de información y geográficos del ambiente de negocios, basados en los principios de negocios sus metas y manejo estratégico • Analizar brechas entre la Línea base y salida de la arquitectura de negocios • Seleccionar los puntos de vista relevantes de la arquitectura que serán habilitados para demostrar como los involucrados están direccionando la arquitectura de negocios • Seleccionar las herramientas relevantes a ser usadas en asociación con los puntos de vista seleccionados

Entregables
a) Procesos de negocio b) Diccionarios de requerimientos de los procesos de negocio c) Línea base de la arquitectura de negocios d) Matriz de asignación de responsabilidades (RACI) e) Arquitectura de negocios

Tabla 25. Fase C: Arquitectura de información

Objetivos
• Desarrollar arquitecturas de salida que cubran ambos dominios: aplicaciones y datos • Definir los mejores tipos y fuentes de datos necesarios para soportar los negocios, de manera que sean comprensibles por los involucrados • Definir las mejores reglas de las aplicaciones de los sistemas necesarios

Objetivos
para procesar datos que soporten los negocios

Entregables
a) Diccionarios de especificaciones funcionales b) Línea base de la arquitectura de las aplicaciones c) Arquitectura de las aplicaciones d) Estructura entidad-relación e) Modelado de datos f) Definición de estructuras de datos g) Línea base de la arquitectura de datos h) Arquitectura de datos

Tabla 26. Fase D: Arquitectura tecnológica

Objetivos
• Determinar los componentes que satisfagan los requerimientos obtenidos de la arquitectura de aplicaciones, de tal forma que sean un conjunto de componentes de tecnología, de software y hardware, disponible en el mercado o configurados dentro de la organización • Definir la realización física de una solución arquitectónica • Definir la Línea base de tecnología, detallando la trayectoria hacia la arquitectura destino, e identificar los paquetes claves de trabajo de la trayectoria

Entregables
a) Línea Base de la Arquitectura tecnológica b) Arquitectura tecnológica

Tabla 27. Fase E: Oportunidades y soluciones:

Objetivos
• Revisar los objetivos y capacidades de la empresa, neutralizar las lagunas de las Fases B, C y D, y organizar grupos de componentes básicos para abordar estas capacidades • Revisar y confirmar los parámetros actuales de la empresa y la capacidad para absorber los cambios • Deducir una serie de arquitecturas de transición que proporcionen un valor empresarial continuo • Generar y obtener un consenso sobre la estrategia de migración

Entregables
a) Versiones afinadas y actualizadas de la Visión de arquitectura, Arquitectura de

Entregables
negocios, Arquitectura de información y Arquitectura tecnológica b) Validación de la arquitectura c) Estados de transición de la arquitectura d) Plan de migración

Tabla 28. Fase F: Plan de migración

Objetivos
• Garantizar que el Plan de migración se encuentre alineado con los diferentes marcos de gestión que se usen dentro de la empresa • Dar prioridad a todos los paquetes de trabajo, mediante la asignación de valor de negocio y llevar a cabo un análisis de costos y de negocios • Finalizar la Visión de arquitectura y arquitecturas producto • Confirmar la arquitectura de transición definida en la Fase E con las partes interesadas • Crear, actualizar y monitorear la información detallada de la ejecución del Plan de migración facilitando los recursos necesarios para permitir la realización de la transición de arquitecturas, tal como se definen en la Fase E

Entregables
• Plan de migración integrado por: • Administración el tiempo: Paquetes de trabajo, cronograma, hitos y ruta crítica • Administración de los riesgos • Administración de los costos • Administración de la comunicación • Administración de los recursos humanos • Actualización de los resultados • Lecciones aprendidas

Tabla 29. Fase G: Gobierno de la implementación

Objetivos
• Formular recomendaciones para la ejecución de proyecto • Elaborar la normatividad para regular el proceso de implementación, y realizar las funciones de gobierno adecuadas, mientras que el sistema está siendo implementado y desplegado • Asegurar la conformidad con la arquitectura definida por el proyecto

Entregables
a) Norma interna para ejercer el gobierno b) Recomendaciones para la ejecución del Plan de migración c) Documentación de la administración del proyecto d) Minutas de trabajo de revisión de avances e) Recomendaciones y acuerdos sobre las medidas para solventar desviaciones de la ejecución del Plan de migración f) Realizar análisis de impacto g) Seguimiento a medidas acordadas en reuniones de revisión previas h) Acta de cierre de la migración

4.2.3 Determinar las herramientas, métodos, técnicas o mejores prácticas que se encuentren en el estado del arte, que serán empleadas en el desarrollo de las fases

Fase B: Arquitectura de negocios

Herramientas, métodos, técnicas, mejores prácticas	Descripción
a) Ingeniería de requisitos	a) Entender el problema, comprender el impacto del sistema en el negocio, que requiere el cliente y cómo interactúan los usuarios del sistema
b) Metodología de la cadena de valor	b) Determinar las actividades de los eslabones de la cadena de valor y de la cadena de soporte **Procesos de su cadena de valor:** **Logística de entrada:** Administración de inventario de materiales **Operaciones:** Procesos preemisión, emisión y postemisión de tarjetas **Logística de salida**: Entrega de producto terminado a clientes, procesamiento de pedidos, programación de pedidos **Mercadotecnia y ventas**: Administración del portafolio de productos, estrategias de los canales de comercialización, levantamiento de pedidos **Servicio:** Atención y soporte a clientes,

Herramientas, métodos, técnicas, mejores prácticas	Descripción
	asesoría a clientes **Procesos de su cadena de soporte**: **Adquisiciones**: Compras de materiales y maquinaria, contratos **Desarrollo tecnológico**: Sistemas de información, monitoreo y seguimiento tecnológico del mercado, participación en comités de estandarización y conformidad. **Administración de recursos humanos**: Reclutamiento, contratación, capacitación y desarrollo de personal **Infraestructura organizacional**: Administración, control de la calidad y mejora continua
c) Estándares de los organismos de estandarización	c) Normas ISO/IEC que aplican
d) Estándares de organismos especializados de la industria	d) Normas Global Platform y EMV que aplican
e) Estándares de la industria de las tecnologías de la información aplicables	e) Normas ISO/IEC, ANSI, IEEE que aplican
f) Inventario de los componentes actuales de la Arquitectura de negocio	f) Integración de la documentación oficial de la empresa

Fase C: Arquitectura de información

Herramientas, métodos, técnicas, mejores prácticas	Descripción
a) Técnicas aportadas por la Ingeniería de la información	a) Técnicas de modelado de datos y aplicaciones
b) Definiciones de los estándares y normas a cumplir	b) Protocolos, procedimientos para la intercomunicación de datos
c) Inventario de las aplicaciones actuales	c) Características, tecnología, interfaces, licenciamiento, personal especializado, soporte y servicio; y componentes especiales.

Fase D: Arquitectura tecnológica

Herramientas, métodos, técnicas, mejores prácticas	Descripción
a) Análisis derivados de la Arquitectura de negocios y de Información: Requisitos funcionales : Producto de las arquitecturas de negocios y de información: Incorporar los requerimientos del SGLL y HSM definidos en DSGLL y DHSM Requisitos no funcionales: Análisis de los impactos del esquema de operación centralizada-descentralizada, Análisis de la compatibilidad con la infraestructura del ambiente de otros sistemas con los que se interconecta, Supuestos Restricciones Dominio específico de tecnología Principios de la arquitectura Políticas Normas Directrices Especificaciones b) TRM de TOGAF	a) Información derivada del conocimiento de la organización, el entorno y la que proporcionen las arquitecturas de negocios e información b) Metodología y base de conocimientos de TOGAF
c) Información del mercado: Estándares y normas de tecnología Cartera de tecnologías Cartera de proveedores Benchmark	c) Información emitida por organismos de estandarización, información de la industria especializada, estudios de mercado comparativo entre tecnologías elaborado por analistas neutrales

Herramientas, métodos, técnicas, mejores prácticas	Descripción
Cuadros mágicos de analistas de tecnología	
d) Matriz SI/Tecnología TRM de TOGAF	d) Correlación entre los SI y sus diversos componentes contra los componentes que ofrece cada tecnología
e) Diagramas de : Ambientes y lugares Descomposición de la plataforma Diagrama de procesamiento Red de comunicaciones	e) Documentación gráfica de todo el ambiente físico
f) Conocimiento del personal	f) Perfiles profesionales, experiencia, habilidades, competencias, entrenamiento, capacitación del personal que se hará cargo de la Arquitectura tecnológica. Así como también la trayectoria y tiempo que se requerirá para que el personal se adapte a la nueva arquitectura
g) Servicios, mantenimiento y outsorcing	g) Evaluación de los proveedores y los servicios que proporcionan
h) Norma ISO/IEC 20000:2005 e ITIL V3.0	h) Mejores prácticas en el otorgamiento de servicios de TI, a través de protocolos de administración de la demanda, administración de la capacidad, administración de los niveles de servicio, administración de la seguridad y la formulación de planes de continuidad del negocio

Fase E: Oportunidades y soluciones

Herramientas, métodos, técnicas, mejores prácticas	Descripción
a) Análisis de brechas entre las arquitecturas	a) Comparativo de los entregables de cada una de las arquitecturas, así como su relación costo/beneficio
b) Diagnostico situacional de los diferentes escenarios de adquisición de la infraestructura, complemento a la actual,	b) Análisis FODA

Herramientas, métodos, técnicas, mejores prácticas	Descripción
adquisición, contratación de servicios.	
c) Administración de proyectos	c) La elaboración del plan de migración determina un conjunto de actividades en el tiempo, que es recomendable programarlos como "paquetes de trabajo", establecer los hitos, los costos asociados, administrar el riesgo y establecer los canales de comunicación

Fase F: Plan de migración

Herramientas, métodos, técnicas, mejores prácticas	Descripción
Mejores prácticas en Administración de proyectos	Marcos de referencia para la Administración de proyectos

Fase G: Gobierno de la implementación

Herramientas, métodos, técnicas, mejores prácticas	Descripción
Mejores prácticas en Administración de proyectos	Marcos de referencia para la Administración de proyectos

4.2.4 A partir de las herramientas seleccionadas obtener los entregables de la fase que corresponda

Fase B: Arquitectura de negocios

La información que aportan los procesos de negocio, requerimientos, especificaciones funcionales, datos, composición de los datos, flujo de datos, medios de almacenamiento y mecanismos de acceso, son documentados en diccionarios de datos, de acuerdo con Gane y Sarson [13], son los medios estructurados que permiten integrar la información relevante para el análisis y diseño de un sistema de información.

a) Definición de los procesos de negocio:

El desarrollo de la AEI requiere determinar los requerimientos que deben de satisfacer las arquitecturas de información y tecnológica. Para tal efecto y tomando en cuenta la visión de la AEI, donde la empresa es el sistema, nos apoyaremos de la Ingeniería del software para obtenerlos. La parte de la Ingeniería del software que realiza esta importante tarea es la denominada Ingeniería de requisitos.

Como lo expresa Pressman [3], la Ingeniería de requisitos

> "proporciona el mecanismo apropiado para entender lo que el cliente quiere, analizar las necesidades, evaluar la factibilidad, negociar una solución razonable, especificar la solución sin ambigüedades, validar la especificación, y administrar los requisitos conforme estos se transforman en un sistema operacional".

Así mismo como lo plantea Ian Sommerville [9], la Ingeniería de requisitos la integran cuatro actividades genéricas de alto nivel:

- El estudio de factibilidad del sistema
- La obtención, el análisis y la documentación de los requerimientos
- La validación de los requerimientos y,
- La administración de los requerimientos

El producto de estas actividades es la especificación de los requerimientos, el cual describe la función y desempeño de un sistema y las restricciones que regirán su desarrollo.

Como lo señala Pressman [3], puede ser un documento escrito, un conjunto de modelos gráficos, un modelo matemático formal, una colección de escenarios de uso, un prototipo o una combinación de estos.

Para los objetivos de esta tesis nos enfocaremos en la obtención, análisis y la elaboración de la especificación y documentación de los requerimientos.

Estas actividades las llevamos a cabo a partir de recurrir a la documentación que refiere el estado del arte que guardan los estándares y normas de la industria, las implementaciones que se han realizado en algunas organizaciones y a trabajos académicos.

La herramienta seleccionada para obtener la especificación de los requisitos de la Arquitectura de negocios es la de cadena de valor. Esta metodología cumple con las características que se requieren para abstraer, conceptualizar y modelar la empresa como un sistema, realizando el modelado de los diferentes niveles, desde su visión de contexto hasta los detalles de los diversos componentes.

Tal como lo señala Michael E. Porter [6],

> "en una organización, se necesita un medio sistemático para examinar todas las actividades que se realizan y su manera de interactuar".

La cadena de valor permite dividir a la organización en sus actividades estratégicamente relevantes a fin de entender su comportamiento.

Las empresas y organizaciones son un conjunto de actividades cuyo fin es diseñar, fabricar, comercializar, entregar y soportar su producto.

Siguiendo con Michael E. Porter [6], las actividades o eslabones de valor se dividen en dos grandes grupos: primarias y de apoyo. Las primeras, son las que intervienen en la creación física del producto. Las de apoyo respaldan a las primarias al ofrecer insumos, tecnología, recursos humanos y diversas funciones globales.

Son cinco las actividades primarias de una cadena de valor:

- Logística de entrada
- Operaciones
- Logística de salida
- Mercadotecnia y ventas
- Servicio

Son cuatro las actividades de apoyo:

- Adquisición
- Desarrollo tecnológico
- Administración de recursos humanos
- Infraestructura organizacional

De acuerdo a Michel E. Porter [6], la descripción de estas actividades es la siguiente:

Logística de entrada: Incluye las actividades relacionadas con la recepción, el almacenamiento y la distribución de los insumos del producto y control de inventario.

Operaciones: Son las actividades mediante las cuales se transforman los insumos del producto final: maquinado, empaquetado, ensamblaje, mantenimiento de equipo, realización de pruebas, impresión y operaciones de planta.

Logística de salida: Son aquellas actividades por las que se obtiene, almacena y distribuye el producto entre los clientes, almacenamiento de producto terminado, manejo de materiales, procesamiento de pedidos y programación.

Mercadotecnica y ventas: Aquellas actividades mediante las cuales se crean medios que permiten al cliente comprar el producto y la compañía inducirlo a ello, publicidad, promoción, fuerza de ventas, cotizaciones, selección de canales, relación entre canales y fijación de precios.

Servicio: Incluye las actividades por las que se da un servicio que mejora o conserva el valor del producto, instalación, reparación, capacitación, suministro de partes y ajuste del producto.

Adquisición: Son las actividades relacionadas con la función de la compra de los insumos, que se emplearan en la cadena de valor.

Desarrollo tecnológico: Toda actividad relacionada que esté relacionada con la tecnología, los procedimientos prácticos, los métodos o la tecnología integrada a los procesos, incluye la tecnología de la información.

Administración de los recursos humanos: Está constituida por las actividades del reclutamiento, la contratación, la capacitación, el desarrollo y la compensación de todo tipo de personal.

Infraestructura organizacional: Las que incluyen la administración general, planeación, finanzas, contabilidad, aspectos legales, normatividad y administración de la calidad

Partiendo de la base de los procesos necesarios para fabricar una tarjeta inteligente, la industria toma como referentes tres etapas para poner en operación una tarjeta en un Programa de tarjetas.

Estas etapas inician con la preemisión, la cual ocurre desde la fabricación del chip hasta que está terminada una tarjeta genérica, es decir tarjetas con todas sus características iguales entre si y que a partir de las actividades de personalización, es cuando cada tarjeta es diferenciada con los datos del titular de la tarjeta, en este momento se puede decir que inicia la etapa de emisión, posteriormente desde el momento en que ocurre la entrega de la tarjeta al titular de la misma hasta su finalización y posible destrucción se contempla la etapa de postemisión.

En la figura 42 se muestra el diagrama de contexto de la producción de una tarjeta inteligente en sus etapas de preemisón y emisión, mientras que en la Figura 43 se muestra el diagrama de contexto de los procesos de postemisión de una tarjeta inteligente. En la tabla 30 se relacionan los procesos y entidades que participan durante el ciclo de vida de una tarjeta inteligente.

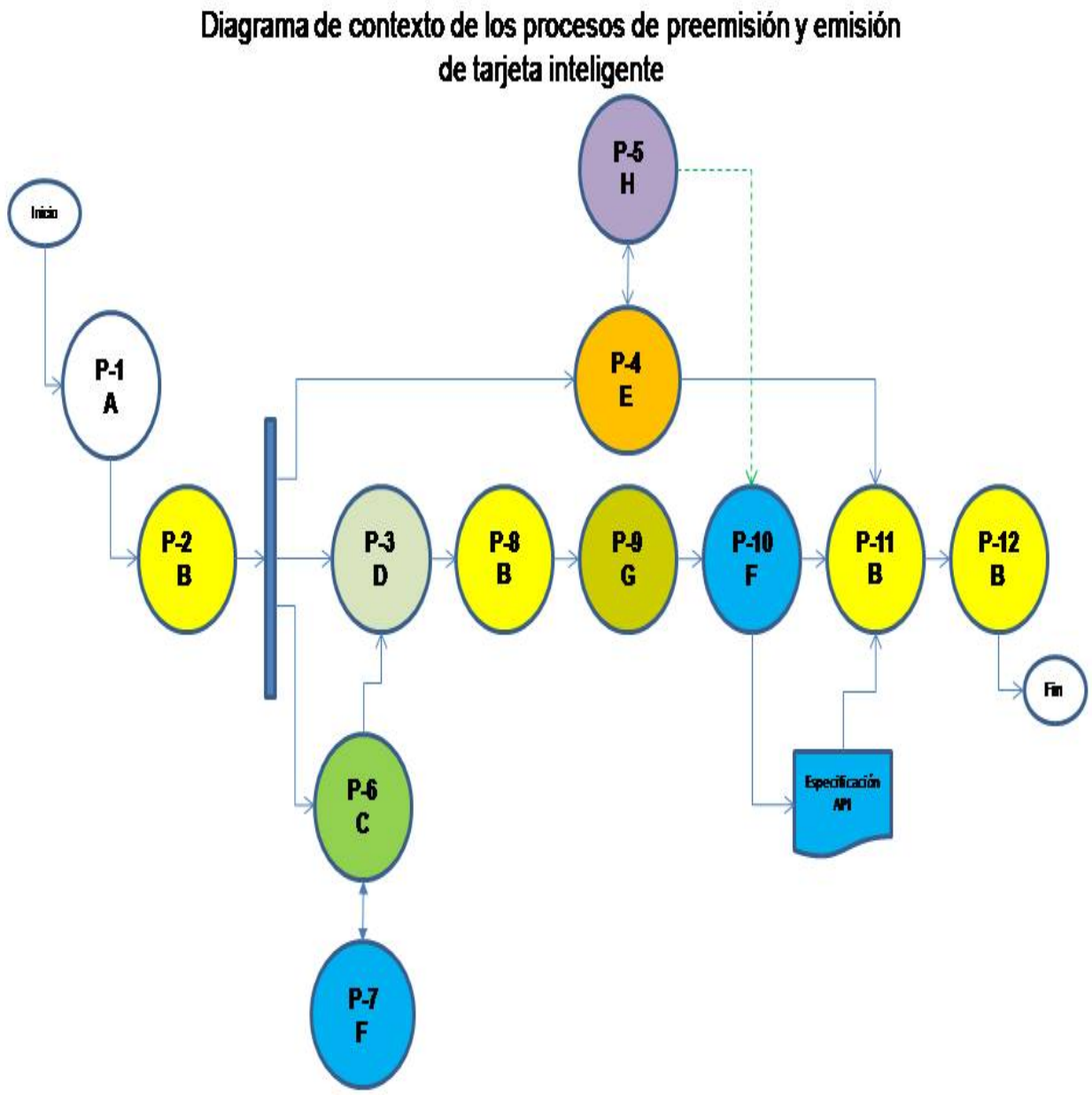


Figura 42. Diagrama de contexto de los procesos de preemisión y emisión de una tarjeta inteligente

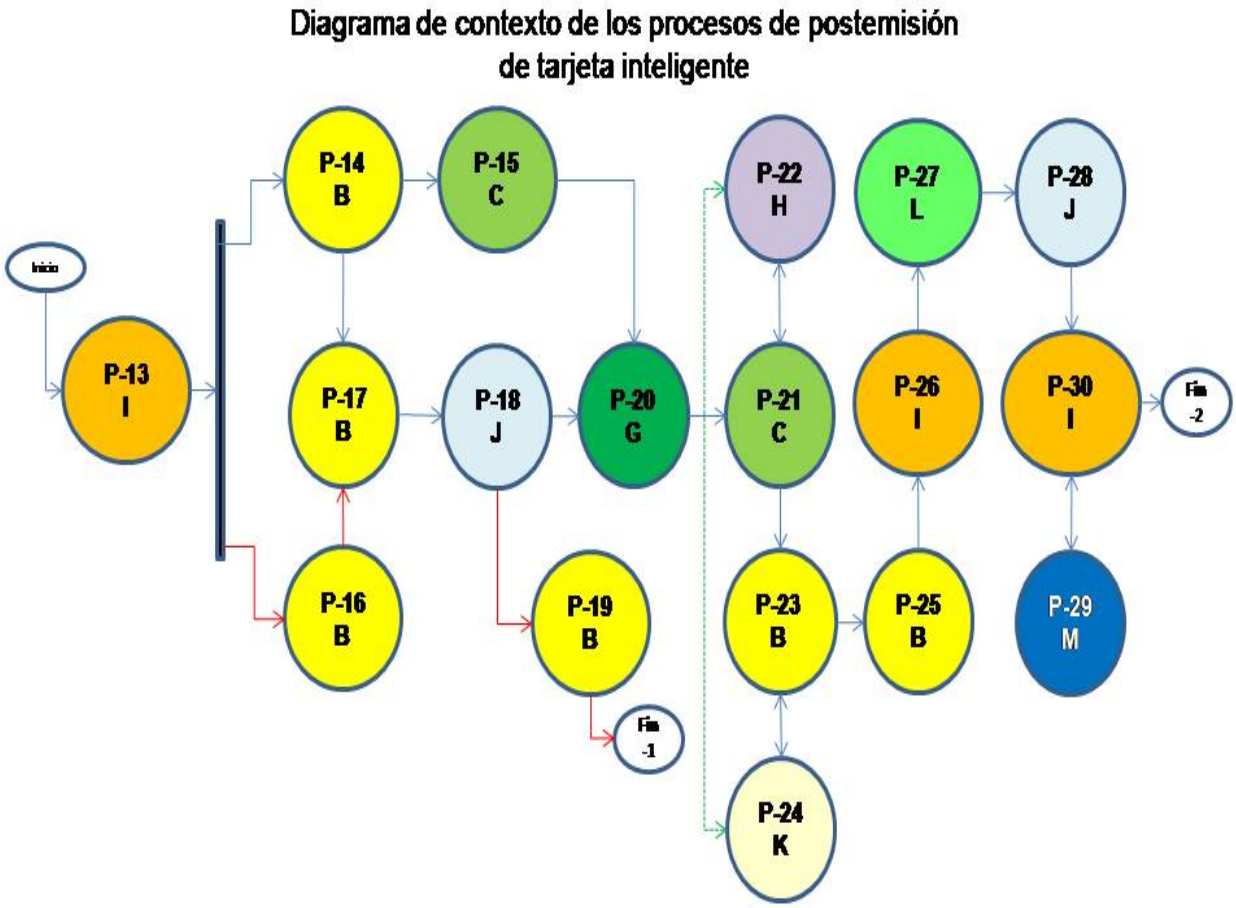


Figura 43. Diagrama de contexto de los procesos de postemision de una tarjeta inteligente

Tabla 30. Procesos y entidades que participan durante el ciclo de vida de una tarjeta inteligente

Proceso
P-1 Solicitud de emisión
P-2 Solicitud de producción de tarjeta, chip y desarrollo de las aplicaciones
P-3 Produce y entrega la tarjeta plástica
P-4 Desarrollo de las aplicaciones

Proceso
P-5 Gestión de las llaves de seguridad
P-6 Produce e inicializa el chip
P-7 Provee la plataforma de desarrollo
P-8 Integra la tarjeta plástica y el chip
P-9 Habilita la tarjeta
P-10 Provee e instala la plataforma y llaves de seguridad
P-11 Carga de las aplicaciones
P-12 Personaliza gráficamente y entrega la tarjeta
P-13 Recibe incidencias sobre la tarjeta inteligente
P-14 Trámita reposición de la tarjeta
P-15 Provee tarjeta para reposición
P-16 Trámita baja de tarjeta de reposición
P-17 Ejecuta baja y bloqueo de la tarjeta que ingresa a lista caliente
P-18 Actualiza listas calientes
P-19 Confirma baja de tarjeta de reposición
P-20 Habilita tarjeta nueva
P-21 Provee e instala plataforma de llaves
P-22 Gestiona llaves de seguridad
P-23 Carga de aplicaciones
P-24 Provee aplicaciones
P-25 Personaliza graficamente y entrega tarjeta nueva
P-26 Recibe tarjeta de reposición y entrega a titular
P-27 Genera transacciones electrónicas
P-28 Colecta datos de transacción
P-29 Soporte a operador de programa
P-30 Concentra transacciones

Entidad empresarial
A: Solicitante
B:Integrador/emisor
C: Fabricante del chip
D:Fabricante de la tarjeta plástico
E: Desarrollador de la aplicación
F: Proveedor de la plataforma del chip
G: Habilitador de la tarjeta
H: Entidad autoridad de control/Certificador
I: Operador del programa
J: Colector de las transacciones
K: Proveedor de las aplicaciones
L: Socio de negocios
M. Buro de servicio

De acuerdo a la cadena de valor, el eslabón de Operaciones contempla los tres procesos referidos, mientras que el eslabón de apoyo Desarrollo tecnológico contempla la administración y soporte del SGTI.

La figura 44 muestra el diagrama de contexto de las cadenas de valor y de soporte, relacionados con los procesos de las etapas de producción de una tarjeta inteligente, resaltando los procesos comunes de las diferentes etapas.

Figura 44. Relación de los procesos de la cadena competitiva y los de producción de una tarjeta inteligente

De acuerdo a los estándares y normas publicadas por los organismos de estandarización y los especializados de esta industria, se encuentran documentadas recomendaciones sobre las especificaciones que deben de cumplir tanto las arquitecturas de las tarjetas como los SGTI.

La publicación de estas especificaciones por Global Plataform [W7], especificación de tarjetas Global Platform [R28] (Global Platform Card Specification), Requerimientos funcionales del sistema administrador de la tarjetas inteligentes [R29] (SCMS Functional Requeriments) y sistema administrador de llaves Global Platform [R30] (Global Platform Key Management Systems), el estándar ISO/IEC 7816-13 [W15] y las recomendaciones de otros autores descritas en el apartado 3.3 de este trabajo, son los referentes que emplearemos para detallar los requerimientos y especificaciones funcionales genéricas de un SGTI.

De manera implícita en los requerimientos en los que se refiera el intercambio y transmisión de datos entre componentes de la tarjeta y de ésta con el exterior se deben de cumplir los estándares que aplican a la seguridad como son los de EMV, ISO/IEC, ANSI e IEEE fundamentalmente, así como los correspondientes comandos APDU del sistema operativo de la plataforma de la tarjeta.

Existen proyectos de implementación documentadas con las especificaciones de Global Platform, tal es el caso del Project on Cities Equipped with I.T en Japon [R21] donde se presentan las bases de la implementación de un SGTI con varios Administradores de tarjeta (Card Manager).

De acuerdo a lo anterior se presenta un resumen de estos requerimientos, los cuales se documentan en diccionarios de requerimientos, los que formarán la Línea base de la arquitectura de negocios.

En la descripción de los requerimientos señalamos el término “ambiente del SGTI”, el cual comprende las actividades manuales y automatizadas, estas últimas son consideradas en las aplicaciones del sistema automatizado, las manuales se deben desarrollar como procedimientos.

En este trabajo cuando nos referimos a un componente de la arquitectura de la tarjeta, del SGTI o del SGLL, enunciaremos su nombre en español, escribiendo enseguida el nombre con el que se le conoce en el medio de la industria o de los torganismos certificadores. Ejemplo Administrador de la tarjeta (Card Manager).

Siguiendo con el orden de la cadena de valor se tiene:

b) Diccionarios de requerimientos de la Arquitectura de negocios

Eslabón de la logística de entrada:

Diccionario 8. DL1 Requerimientos del subproceso: Soporte a procesos de negocios: Administración de inventario de tarjetas

El costo de una tarjeta multiaplicativa de gama alta comparada con una tarjeta de banda magnética es significativo. Por esta razón, es importante que el ambiente del SGTI administre la distribución e inventarios de la tarjeta.
La definición de los requerimientos funcionales para la Administración del inventario estan referidos en el Diccionario EL1.

Eslabón de la operación:

Diccionario 9. DO1 Procesos de producción

Procesos productivos	Descripción
Preemisión de la tarjeta	Se refiere a los procesos que se requieren para crear las tarjetas y las aplicaciones, configurar los productos del portafolio y preparar cualquier ambiente que sea necesario para habilitar la emisión de las tarjetas.
Emisión de la tarjeta	Se refiere a los procesos requeridos para producir tarjetas inteligentes personalizadas, incluyendo la habilitación de tarjetas inteligentes sin personalizar, recibidas directamente de los fabricantes de tarjetas.
Postemisiónde la tarjeta	Se refiere a los procesos requeridos para manejar tarjetas inteligentes personalizadas y para ejecutar cualquier cambio en la tarjeta, si ésta ha sido personalizada y emitida al titular de la misma.

Es importante notar que mientras la funcionalidad de la gestión del ciclo de vida de la tarjeta y sus aplicaciones se describe únicamente en la fase de postemisión, estos son requerimientos funcionales que aplican tanto a los procesos de preemisión y emisión. Por simplificación, estas dos áreas de funcionalidad están categorizadas como procesos de postemisión, como la fase en la cual todos los requerimientos funcionales serán aplicables.

A la inversa, la funcionalidad principal soporta estos procesos mayores y son agrupados de acuerdo a las áreas de funcionalidad, gestión de llaves, administración y mantenimiento de la arquitectura del sistema.

De acuerdo con la nomenclatura de los procesos de negocio o requerimientos están presentados en la figura 45 como procesos de preemisión, emisión y postemisión, mientras que los procesos de soporte están señalados como de funcionalidad básica.

La descripción de los requerimientos de los procesos de negocio se refleja en los siguientes diccionarios,

Procesos de preemisión de la tarjeta

Antes de emitir una tarjeta personalizada, las características de la tarjeta requerida deben de ser definidas, esto de acuerdo a los perfiles:

- Del microprocesador
- La tarjeta
- Las aplicaciones y,
- La seguridad

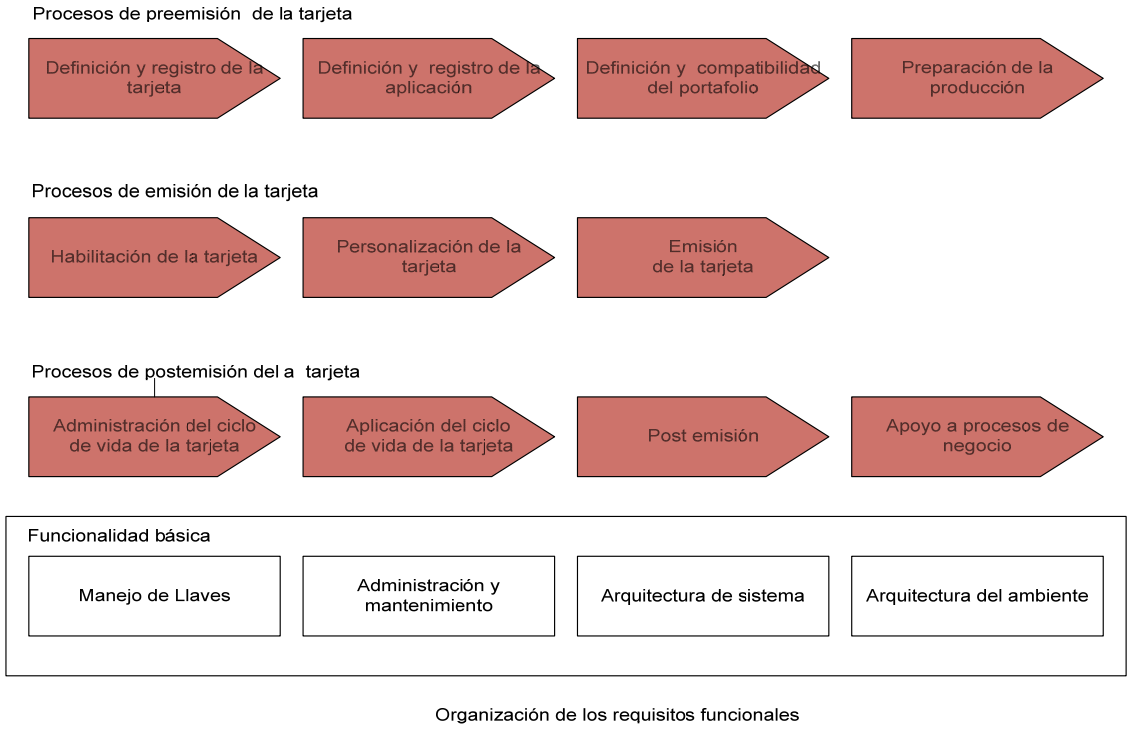


Figura 45. Procesos de producción de una tarjeta inteligente

Una vez que los atributos de la tarjeta y las aplicaciones son registradas en el ambiente SGTI, el portafolio de producto puede ser creado y las compatibilidades técnicas y de negocio pueden ser evaluadas. Para productos válidos, el paso final en preemisión implica preparar los componentes del ambiente del SGTI necesario para la producción. La figura 46 representa los subprocesos de la etapa de preemisión de la tarjeta.

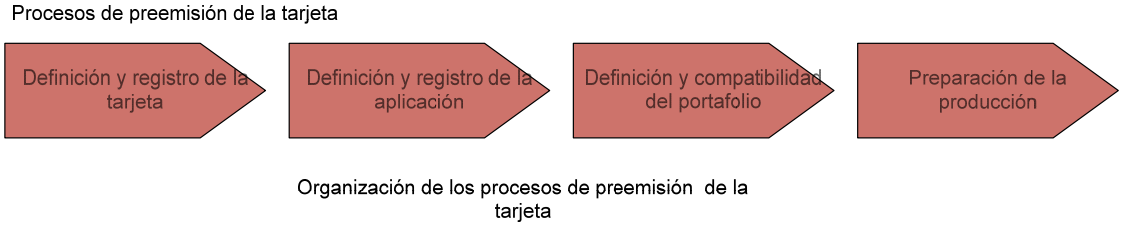


Figura 46. Cadena de valor de la etapa de preemisión

Diccionario 10. DO2 Requerimientos de los subprocesos de preemisión

Proceso: Preemisión	**Subprocesos**
	Definición y registro de la tarjeta
	Definición y registro de aplicaciones
	Definición y compatibilidad de portafolio (cartera)
	Preparación de la producción

Diccionario 11. DO3 Requerimientos del subproceso: Definición y registro de la tarjeta

Existen numerosos tipos de tarjetas y ambientes de ejecución. Durante el aprovisionamiento de la tarjeta, un emisor necesitara realizar la selección asegurándose de las necesidades actuales y futuras.

Los atributos de las tarjetas disponibles para la selección, deberán de ser listados en los diccionarios de perfiles del ambiente del SGTI. El perfil de la tarjeta es una descripción del hardware requerido y del ambiente operativo para un chip específico. El perfil contiene información detallada acerca del chip, información del fabricante, versión, capacidades del procesador del chip, capacidad de memoria (EEPROM, RAM, ROM), sistema operativo, ambiente de ejecución y el conjunto de aplicaciones presentes en el chip.

El perfil de la tarjeta puede ser usado para proporcionar una vista instantánea de una tarjeta inteligente, así como la evolución que ocurre desde que se encuentra en la etapa de fabricación hasta que la posee el titular de la tarjeta.

En [W24], [W25], [W26], [W27] y [W28] se encuentran publicadas fichas técnicas de chips y microprocesadores.

En el Diccionario EO3 están mapeados los requerimientos funcionales para administrar los perfiles de las tarjetas.

Diccionario 12. DO4 Requerimientos del subproceso: Definición y registro de las aplicaciones

El perfil de una aplicación es una descripción de los recursos necesarios, elementos de datos, procesos y privilegios para una aplicación específica. La información de los perfiles de las aplicaciones incluye requerimientos de datos y llaves, definición de procesos para los pasos lógicos y los comandos necesarios para la inicialización y la personalización de las aplicaciones.

El ambiente del SGTI debe de ser diseñado para atender la administración distribuida de aplicaciones, para evitar colocar la carga completa en la administración del emisor. Como resultado de esto, el perfil de las aplicaciones incluye referencias de la ubicación del código de la aplicación mediante el perfil del archivo de carga e incluye la especificación de las llaves relacionadas con la aplicación.
El ambiente del SGTI integrará el Diccionario de requerimientpos funcionales EO4 para administrar los perfiles de las aplicaciones:

Como se ha referido en el apartado 2.7 de este trabajo, el Administrador sería representado como otro perfil de aplicación. Los requerimientos específicos o privilegios de la aplicación Administrador, que el ambiente SGTI debe ser capaz de ejecutar son:

- Almacenar los privilegios de la aplicación Administrador. Estos privilegios determinan si la aplicación es seleccionada por default, si puede cambiar el Pin Global o bloquear el Administrador de la tarjeta (Card Manager)

- Almacenar los requerimientos de la aplicación Pin (ninguno, local o global) y administrar las reglas de negocio relativas al cambio del Pin.

Diccionario 13. DO5 Requerimientos del subproceso: Definición y compatibilidad del portafolio (cartera)

La salida del perfil de tarjetas y aplicaciones dicta el conjunto de requerimientos del diccionario DO5 del ambiente SGTI, los cuales son la definición del portafolio primario y aseguran la compatibilidad de este portafolio con las reglas técnicas y de negocios.

Antes de emitir las tarjetas inteligentes multiaplicativas, el emisor deberá definir las aplicaciones primarias o las mezclas iníciales de aplicaciones en la tarjeta. El portafolio primario puede consistir de un conjunto de aplicaciones fijas con un conjunto de aplicaciones opcionales.

Basado en el perfil de la tarjeta y el perfil primario de aplicaciones, el emisor puede manejar opciones sobre la memoria disponible para descargas en postemisión.

Un emisor debería siempre tener la idea de que aplicaciones en etapa de postmisión podrán ser descargadas, los perfiles de estas aplicaciones deberán de ser proporcionadas para asegurar que todos los componentes necesarios estén presentes y no existan problemas con la integridad del perfil de la tarjeta.

El emisor necesita una lista de perfiles, para poder seleccionar una tarjeta específica, que cumpla los requerimientos para un perfil particular de producto

El emisor deberá de decidir sobre las aplicaciones primarias de la tarjeta.

El ambiente del SGTI deberá determinar automáticamente si los requerimientos de memoria y criptografía para la mezcla de aplicaciones son idóneos o están en conflicto con el perfil de tarjeta elegido. Alternativamente, el ambiente del SGTI deberá de ser capaz de calcular un apropiado perfil de tarjeta en términos de tamaño y requerimientos de ejecución para el conjunto de aplicaciones mezcladas.

Gran parte de este trabajo es realizado de manera independiente manual o automatizado por los fabricantes del chip y la tarjeta, es prudente que el ambiente del SGTI tenga control de estos datos para estar en condiciones de habilitar la descarga de aplicaciones en postemisión. Esta capacidad podría también proveer facilidades en la selección de fuentes alternativas para sustituir por nuevas tarjetas o reemitir tarjetas.

El Diccionario de requerimientos funcionales EO5 establece la definición del portafolio.

Es necesario realizar controles a tarjetas que existen, aplicaciones y definiciones del portafolio para asegurar que las aplicaciones requeridas puedan caber dentro de las limitaciones del chip, y que puedan de manera segura ser descargadas y funcionar correctamente sobre una tarjeta inteligente en particular. Estos controles pueden ser ejecutados en tarjetas individuales o a través de un rango de tarjetas.

Estos controles pueden tomar lugar en el momento de que la descarga es requerida o un conjunto de aplicaciones pueden ser preverificadas para un rango de tarjetas.

Incluso si ellos no son siempre definidos en las tarjetas o aplicaciones, los requerimientos técnicos para control de compatibilidad a ser ejecutados en el ambiente del SGTI deben de comprobarse.

Los requerimientos funcionales de la compatibilidad del portafolio, están referidos en el Diccionario EO6.

Las solicitudes de las aplicaciones necesitan ser validadas a partir de las reglas de negocios establecidas por el emisor, y cada regla de negocios puede ser compleja dependiendo de las reglas del ciclo de vida.

La razón de que en varias reglas de negocios usualmente surgen problemas, es como resultado de alguno de los siguientes factores:

- Segmentación de la marca
- Conflictos de seguridad
- Riesgo de conflictos del emisor
- Conflictos legales de propiedad y,
- Elegibilidad del titular de la tarjeta para la aplicación

Diccionario 14. DO7 Requerimientos del subproceso: Preparación para la producción

Ordenar la información de la tarjeta inteligente, deberá de ser compilada desde la salida de la decisión del chip y del proceso de selección del portafolio primario.

Esta información deberá de ser enviada al fabricante de la tarjeta. El fabricante de la tarjeta puede en muchos casos también ser una entidad que integre información de los módulos del chip para la habilitación del rendimiento de la tarjeta.

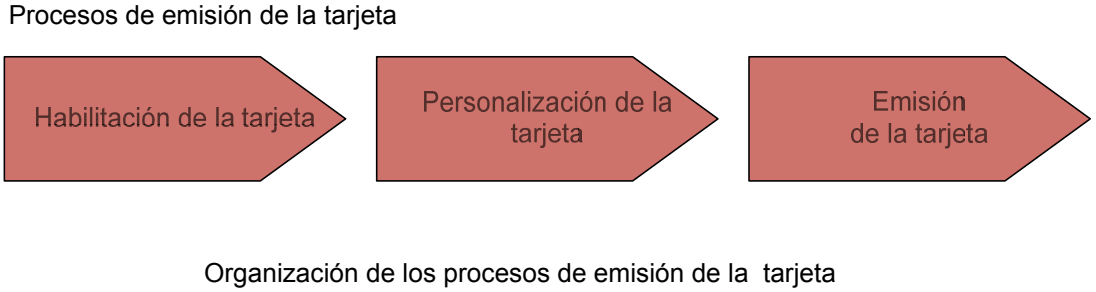
Sin embargo, durante el proceso de abastecimiento de la tarjeta, se puede requerir directamente al fabricante del circuito integrado, especialmente, si hay un conjunto de especificaciones para el desarrollo de la máscara. Además, en muchos casos, el proveedor del chip derivara una llave maestra que depende directamente del fabricante de la tarjeta.

Las actividades de este subproceso tienen interacción e interfaz con el sistema de gestión de llaves (SGLL) como se ha referido en el apartado 3.5.2 de este trabajo.

Basados en las relaciones de negocios entre el fabricante del circuito integrado y el fabricante de la tarjeta, el ambiente del SGTI deberá de ser capaz de administrar los requerimientos funcionales expresados en el Diccionario EO7

Diccionario 15. DO8 Requerimientos de los procesos de producción de la tarjeta

Una vez que las aplicaciones iníciales o primarias están definidas y la base de datos primaria de titulares de tarjetas está integrada, una tarjeta acorde a los requerimientos del cliente es seleccionada y seleccionado el diseño de la tarjeta, el paso siguiente es el lanzamiento de un Programa de tarjeta Inteligente multiaplicativa. Este proceso de producir la tarjeta personalizada incluye algunos subprocesos mayores. Los requerimientos son agrupados de acuerdo a estos sub procesos y están señalados en la figura 47.



Organización de los procesos de emisión de la tarjeta

Figura 47. Cadena de valor de las etapas de emisión

Diccionario 16. DO9 Requerimientos del subproceso: Habilitación de la tarjeta

La Habilitación de la tarjeta es definida como el proceso de cargar los datos y llaves iníciales en el Administrador de la tarjeta (Card Manager), instalando y complementando los dominios de seguridad (Security Domains) y cargando las llaves iníciales en los dominios de seguridad.

La Habilitación usualmente ocurre con el fabricante de la tarjeta, y las aplicaciones pueden opcionalmente ser cargadas e instaladas durante este proceso.

La Habilitación de la tarjeta personaliza el dominio de seguridad del Emisor con las llaves derivadas del dominio de seguridad. Las llaves de los dominios de seguridad son típicamente proporcionadas por el proveedor de aplicaciones.

El segundo paso en el proceso de producción de la tarjeta es la personalización, el cual consiste en la carga, instalación y personalización de las aplicaciones.

Este paso puede ser combinado con la Habilitación de la tarjeta en un proceso ejecutado por una entidad que puede ser el fabricante de la tarjeta o un despacho de operación. La decisión para combinar la Habilitación con la Personalización en una implementación específica que impacta a las aplicaciones, los requerimientos de distribución y el equipamiento para la personalización, puede ser determinada por el fabricante de la tarjeta.

La preparación de datos del sistema en el ambiente del SGTI ejecuta una parte del proceso de Habilitación para derivar las llaves necesarias desde la llave maestra inicial del emisor. Esta actividad es de particular importancia si el ambiente del SGTI es usado en un despacho de operación.

En el Diccionario EO9 se detallan los requerimientos funcionales generados por las actividades de Habilitación de la tarjeta.

Diccionario 17. DO10 Requerimientos del subproceso: Personalización de la tarjeta

Como se ha citado anteriormente, es posible y en algunos casos es recomendable, combinar la carga y personalización de las aplicaciones del portafolio primario en la Habilitación de la tarjeta y los dominios de seguridad.

La Personalización de la tarjeta es definida como el proceso por medio del cual un conjunto específico de aplicaciones son seleccionadas y son provistos los datos específicos para cada titular de tarjeta. La Personalización de la tarjeta es por lo tanto asignar aplicaciones específicas para cada una.

La Personalización de la tarjeta también requiere la generación del Número de Referencia de la tarjeta (CRN por sus siglas en ingles) y del Número de Imagen de la Tarjeta (CIN).

El CRN es un número lógico que está fuera de la tarjeta, que identifica el conjunto de aplicaciones asociadas con una tarjeta y liga estas al titular de la tarjeta.

El CRN sigue siendo válido para el titular durante la vida de la tarjeta. A la inversa el CIN es un número dentro de la tarjeta, que está escrito en ella y puede ser usado como un dato derivado. El CIN sigue siendo válido durante la vida de la tarjeta.

En resumen para cargar y personalizar aplicaciones, el Cargador de aplicaciones (Applications Loader) necesita personalizar el Administrador de la tarjeta y las llaves del dominio de seguridad.

Estas llaves son siempre derivadas, independientemente por el Emisor o el Proveedor de aplicaciones para asegurar que, tras la emisión, únicamente el emisor tenga acceso a la llave maestra final del Administrador de la tarjeta y únicamente el proveedor de aplicaciones tenga acceso a la llave maestra final del dominio de seguridad.

La funcionalidad deberá también existir para llevar a cabo la preparación de datos y personalización de los scripts para el sistema de Información relacionado con la preparación de datos y los dispositivos de carga de aplicaciones. El archivo de datos preparado y scripts asociados podrían ser enviados al despacho de

personalización, al dispositivo de inicialización de la emisión o en algunos casos al fabricante de la tarjeta.

Debe observarse que el Proveedor de aplicaciones es el responsable de recuperar y generar los datos apropiados de personalización. El ambiente del SGTI o sistema de información para la preparación de datos combina los datos desde varias aplicaciones en un solo archivo para el dispositivo de personalización.

Un equipo para la personalización típicamente acepta únicamente un archivo para preparación de datos y un conjunto relacionado de instrucciones, los cuales necesitan una colección previa y preparación de todos los datos requeridos para la personalización. En el sitio [W41] se publican los principales equipos de personalización. La Preparación de datos se ilustra en la figura 48 y la Personalización de datos en la figura 49, según recomendaciones de Global Platform.

La Preparación de datos de la aplicación y de las llaves, deberá ser provista por un sistema separado con una interfaz al ambiente del SGTI, o por una funcionalidad del propio ambiente del SGTI. Las actividades y recomendaciones para esta parte del proceso fueron documentadas en el apartado 3.6 de este trabajo.

Los propósitos generales del ambiente SGTI para los requerimientos funcionales de Personalización se listan en el Diccionario EO10

En adición a las aplicaciones del chip, en la personalización, ésta puede incluir codificación de la banda magnética, imprimir y embozar la tarjeta con información del titular del mismo. El ambiente del SGTI o el sistema relacionado para la preparación de datos deberá idealmente gestionar ambos procesos de personalización. Usualmente la personalización que no pertenece al chip es ejecutada por otro sistema, el cual puede ser con hardware específico.

El Diccionario EO11 establece los requerimientos funcionales para actividades posteriores al subproceso de personalización.

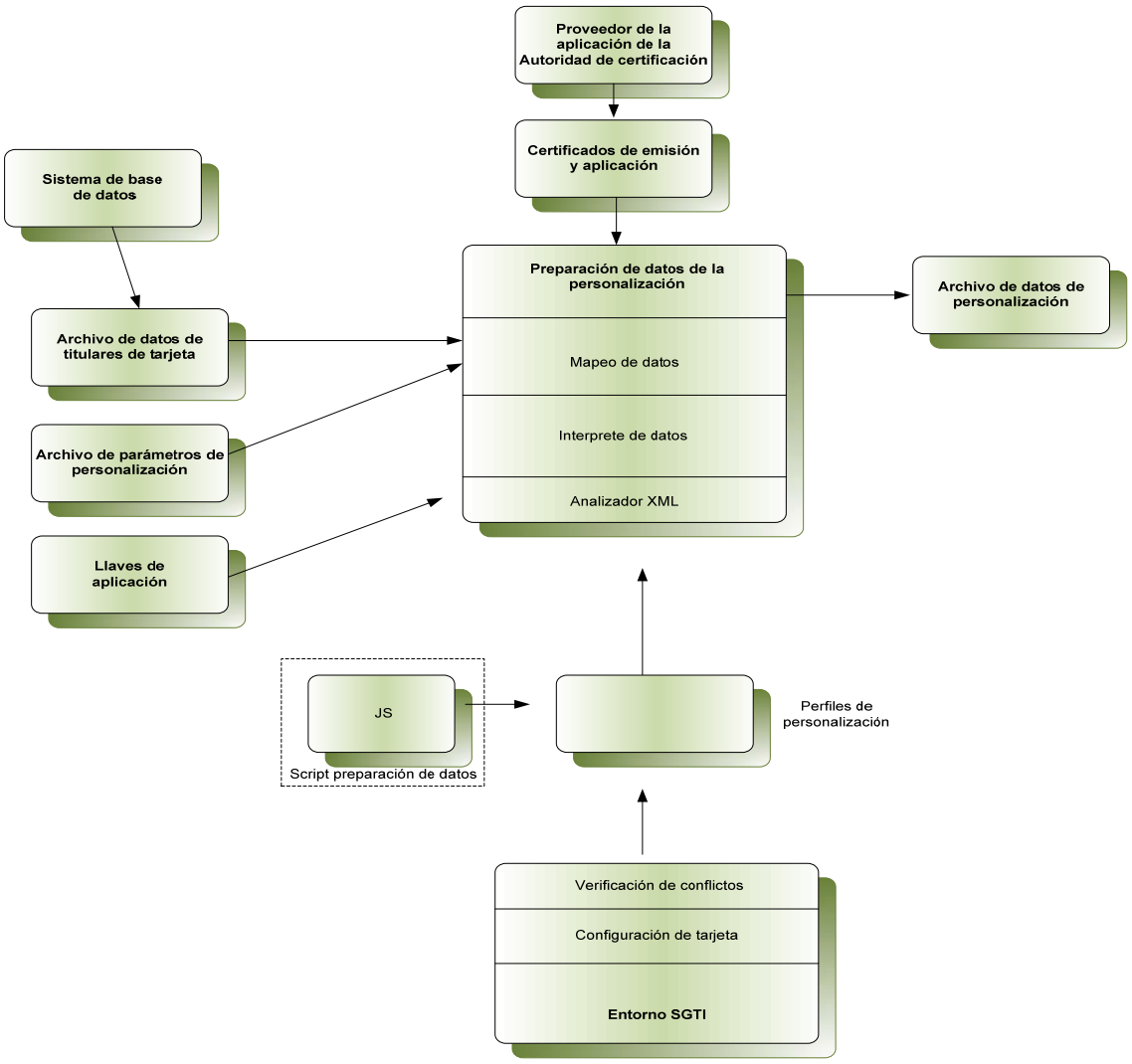


Figura 48. Flujo para la preparación de los datos

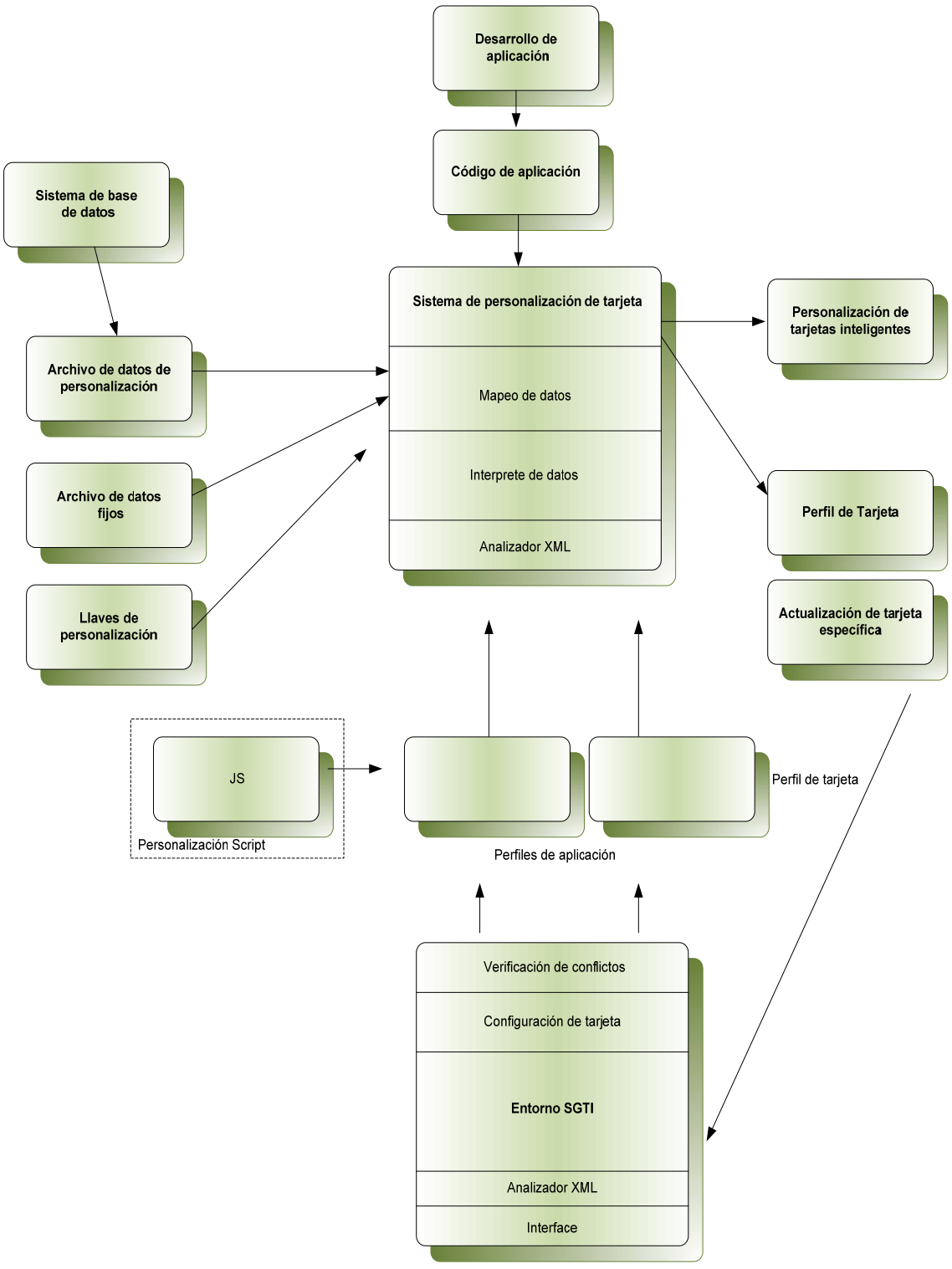


Figura 49. Flujo para la personalización de las tarjetas

Diccionario 18. DO12: Requerimientos de la terminación de la producción de la tarjeta

Dependiendo de las aplicaciones primarias y de las aplicaciones de los proveedores, la tarjeta y su contenido pueden necesitar ser asociados con las transacciones de aplicaciones específicas y sistemas de información de los clientes. En algunos casos la asociación puede ser una liga a la base de datos del emisor o a sus aplicaciones de bases de datos. La definición de la interfaz y datos requeridos dependen de la naturaleza de la aplicación especifica y cualquier nivel de servicio negociado entre el emisor y el proveedor de aplicaciones.

Dependiendo de estos requerimientos, alguna información del cliente deberá de ser replicada en el ambiente del SGTI como un perfil del cliente por separado.

Como especificación general, el ambiente del SGTI deberá de manejar el perfil del cliente.

El Diccionario EO12 expresa los requerimientos funcionales de la terminación de la producción de la tarjeta.

Procesos de producción postemisión de la tarjeta

Hay requerimientos funcionales específicos que son pertinentes para la gestión general de la tarjeta y deberán de ser incluidas como requerimientos para la administración de tarjetas multiaplicativas. Los requerimientos del ciclo de vida de las aplicaciones y la tarjeta son descritas en esta sección y son válidas para la preemisión y procesos de emisión.

Diccionario 19. DO13: Requerimientos de los procesos de producción postemisión

Proceso: Producción Postemisión	**Subprocesos**
	Gestión del ciclo de vida de la tarjeta
	Aplicación del ciclo de vida de la tarjeta
	Postemisión
	Soporte a procesos de negocio

Los procesos involucrados en la producción postemisión son resumidos en la figura 50

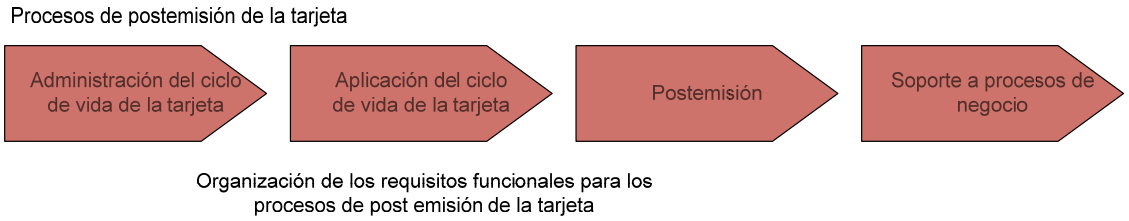


Figura 50. Cadena de valor de la etapa de postemisión

Un aspecto básico de interés, es si el emisor permite carga dinámica y borrado de aplicaciones en postemisión. Durante la postemisión, hay ciertos procesos y funcionalidad dinámica que necesita ser considerada para tener un efectivo ambiente de SGTI. Finalmente, en adición al soporte de requerimientos específicos de personalización en postemisión, existen varios componentes operacionales del ambiente del SGTI.

Los requerimientos funcionales para estos componentes son agrupados bajo la categoría de soporte de procesos de negocio, también son aplicables a los procesos de preemisión y emisión de la tarjeta, aunque ellos son típicamente más utilizados una vez que la tarjeta ha sido accesada.

El ambiente del SGTI normalmente no requerirá proveer procesamiento de transacciones de las aplicaciones incorporadas al sistema. En otras palabras, los sistemas de información que administran las transacciones de las aplicaciones de la tarjeta deberán de estar dispuestos a correr independientemente del ambiente SGTI. Hay dos importantes excepciones a esta premisa:

- Aplicaciones de sistemas que generan cambios en los estados del ciclo de vida de las aplicaciones y la tarjeta. Estos cambios pueden ocurrir cuando una aplicación del sistema detecta algún tipo de fraude

- Interfaces en los sistemas de soporte de los clientes. La aplicación del proveedor puede iniciar una tarjeta o transición del ciclo de vida de la aplicación

La interacción e interfaces del SGTI con otros SI, están referidos en los apartados 3.6 y 3.7 de este trabajo.

Diccionario 20. DO14 Requerimientos del subproceso: Gestión del ciclo de vida de la tarjeta

Las recomendaciones relativas a los procesos de los estados del ciclo de vida de la tarjeta según ISO/IEC 10202 [W15] y GP [W7] están expresadas en el apartado 2.5 de este trabajo. Aquí se reproducen en la tabla 31 y figura 51.

Tabla 31. Ciclo de vida de acuerdo a la norma ISO/IEC 10202-1

Fase	Descripción de la fase del ciclo de vida de la tarjeta	Actividades típicas
1a	Producción del chip y la tarjeta inteligente	Diseño del chip Generación del sistema operativo de la tarjeta Fabricación del chip y módulos de hardware Producción del cuerpo de la tarjeta Embebido del chip en el cuerpo de la tarjeta
2a	Preparación de la tarjeta	Complementación del sistema operativo de la tarjeta
3a	Preparación de las aplicaciones	Inicialización de aplicaciones Personalización de aplicaciones, visual y eléctrica
4a	Uso de la tarjeta	Activación de aplicaciones Desactivación de aplicaciones
5a	Terminación del uso de la tarjeta	Desactivación de aplicaciones Desactivación de la tarjeta

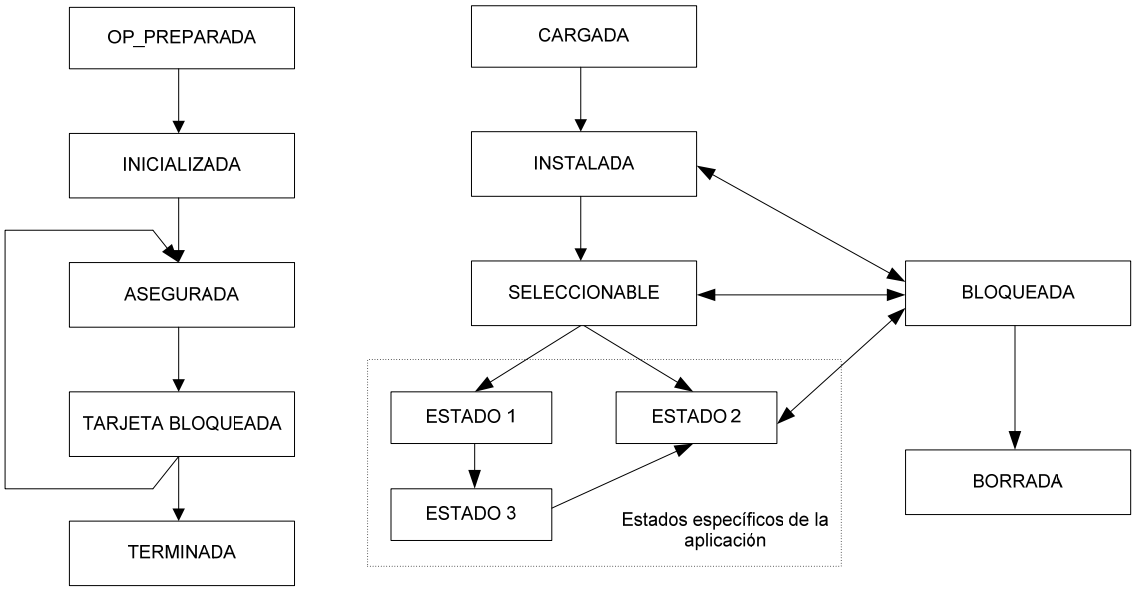


Figura 51. Ciclo de vida de las tarjetas y las aplicaciones

El diccionario EO14 establece los requerimientos funcionales del subproceso gestión del ciclo de vida de la tarjeta.

Un ejemplo de implementación del ciclo de vida se documenta en el National Smart Card Framework del Gobierno de Australia [R24], en el documento Australian Government Interoperability Frameworks [R25] y en el documento Smart Card Project Design Guide [R26] y [W40].

Diccionario 21. DO15 Requerimientos del subproceso: Gestión del ciclo de vida de las aplicaciones

Si fuera el caso de que la tarjeta tuviera aplicaciones EMV, el ambiente del SGTI y en su caso el emisor (perteneciente a la industria financiera) deberá de dar seguimiento a los estados del ciclo de vida de la tarjeta y las aplicaciones, independientemente de cada una de las variantes, para otro tipo de aplicaciones por parte de otros emisores que requieren también conocer los diferentes estados en que se encuentran las aplicaciones, en términos de vigencia, de actualización en postemisión, carga de nuevas aplicaciones o eventos relacionados con la pérdida y por lo tanto reposición de la tarjeta con el último estado de las aplicaciones.

El ambiente del SGTI deberá de dar seguimiento, mantener y reportar los estados de los ciclos de vida.

En el apartado 2.5.3 se describió las características de estos procesos.

La definición de los requerimientos funcionales del ciclo de vida de las aplicaciones se expresa en el Diccionario EO15.

Diccionario 22. DO16 Requerimientos de interfaces con otros sistemas

El ambiente del SGTI deberá de ser interfaz con sistemas existentes fuera de la tarjeta. Estos requerimientos son necesarios en áreas como logística de entrada, logística de salida, servicio y soporte al cliente. También es importante, que el ambiente del SGTI deba de transmitir aplicaciones o estados de los cambios de la tarjeta a las aplicaciones de los sistemas que reciban las actualizaciones de la tarjeta o estados de las aplicaciones.

La interacción e interfaces que tiene el SGTI con otros SI fueron revisados en los apartados 3.3, 3.6 y 3.7.de este trabajo.

Los requerimientos listados en el Diccionario EO16 pueden ser implementados en un SGTI integrado o en sistemas separados que comprendan el ambiente del SGTI.
Una lista caliente, es una lista de tarjetas o aplicaciones que deberán de ser deshabilitadas para su posterior uso. Las tarjetas pueden ser puestas en una lista

caliente por varios motivos de negocios. El ambiente del SGTI puede ofrecer la funcionalidad de listas calientes definidas en los siguientes requerimientos:

- Administrar el procesamiento de las respuestas a las listas calientes que actualizan el estado de la tarjeta, una aplicación o de ambos
- Distribuir esta información a las aplicaciones de los sistemas con los que tiene interacción
- Preparar listas calientes para descargar aplicaciones operacionales de sistemas, de terminales o servidores principales
- Administrar la distribución de listas calientes para aplicaciones de sistemas operacionales, dispositivos o servidores principales y el resultado de las notificaciones desde aplicaciones de sistemas operacionales, dispositivos o servidores centrales

Subproceso: Postemisión

La especificación de las tarjetas está diseñada para permitir que un emisor pueda cambiar el contenido de las tarjetas emitidas al titular de la misma. El proceso de postemisión involucra algunos factores de negocios, operacionales y técnicos que no son requeridos durante los procesos de producción de la tarjeta.

La figura 52 muestra la visión de alto nivel de la infraestructura de descarga, según Global Platform [W7].

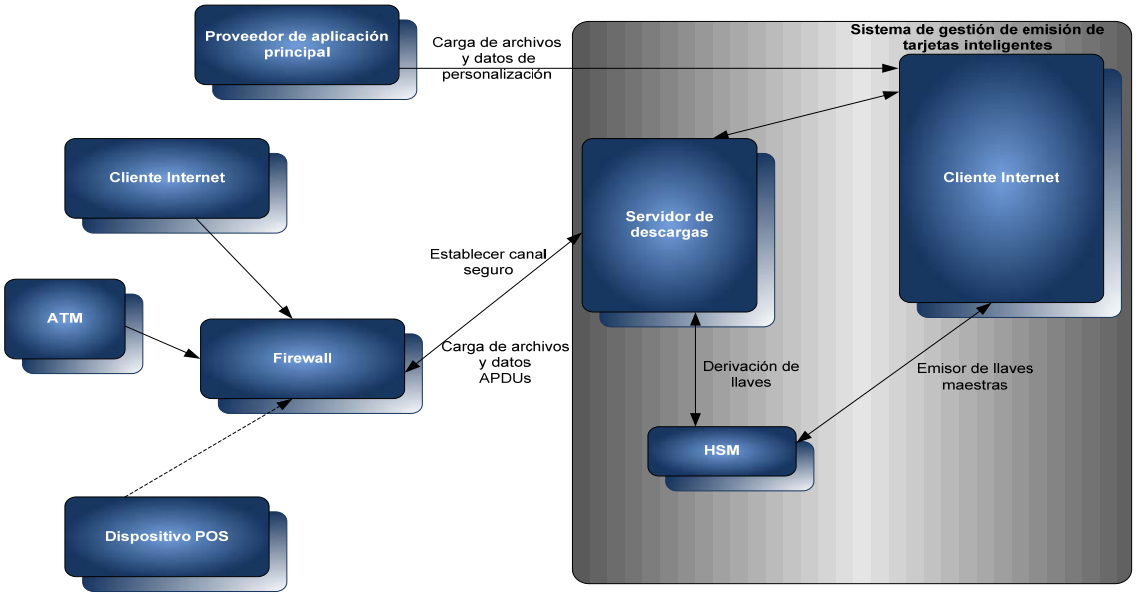


Figura 52. Infraestructura de descarga de aplicaciones en etapa de postemisión

Desde la visión de negocios y aspectos operacionales, el emisor puede administrar directamente todos los cambios o delegar algunos controles al socio de negocios, tal como puede ser el proveedor de aplicaciones.

La descarga de aplicaciones y el compartir responsabilidades en la administración de aplicaciones por terceras partes es llamada Administración delegada. Esto proporciona al emisor un método seguro de permitir que un proveedor de aplicaciones, operador de la plataforma o socio de negocios ejecute el control de la gestión de los contenidos de las tarjetas emitidas. El control de la gestión de contenidos ocurre usando dominios de seguridad adicionales con la delegación de la gestión de privilegios especificada.

Desde la perspectiva técnica, la carga de archivos y la gestión del ciclo de vida necesitan ser consideradas. Primero, se requiere la preparación de archivos de carga que son transferidos a las tarjetas para actualizar el contenido de las tarjetas. Los archivos de carga pueden ser protegidos por bloques patrón de datos de autenticación, los cuales verifican la integridad de los archivos de carga.

Segundo, para concluir los procesos de carga e instalación deberán de ser comunicados al ambiente del SGTI con la correspondiente actualización a los ciclos de vida de la tarjeta y de las aplicaciones.

Los requerimientos que soportan las descargas en postemisión de aplicaciones son divididos en algunas categorías:

Para descarga de aplicaciones, estas categorías son:

- Funcionalidad general para descarga de aplicaciones, incluyendo infraestructura y control de compatibilidad del portafolio de aplicaciones
- La postemisión puede ocurrir en diferentes canales, cada cual puede tener requerimientos específicos
- Requerimientos de seguridad para la descarga de manera segura de las aplicaciones
- El ambiente de postemisión es sujeto a la fiabilidad de la infraestructura de las comunicaciones y a la ocurrencia de errores durante la descarga de aplicaciones. También, la recuperación completa de tarjetas puede ser requerida
- Para programas más sofisticados, la gestión delegada es un recurso que las tarjetas pueden soportar
- Como la participación del titular de la tarjeta es necesaria, puede ser requerido habilitar la descarga de aplicaciones o la recuperación de las tarjetas, la usabilidad de la solución deberá de ser considerada, para proporcionar certeza a todo el programa

Diccionario 23. DO17 Requerimientos de subprocesos: Postemisión: Descarga de aplicaciones

Dependiendo de la arquitectura y distribución de los servidores de carga, una interfaz entre uno o más servidores de carga de las aplicaciones y el ambiente del SGTI puede ser requerida. Esta interfaz deberá permitir transmitir información de manera segura desde la tarjeta al ambiente del SGTI. Para programas cerrados o de poco volumen, el ambiente del SGTI puede actuar como el servidor de carga de aplicaciones.

Independientemente de la arquitectura, ésta deberá de ser el mecanismo para administrar los procesos de descarga de las aplicaciones con una ventana factible de tiempo. Descargas completamente exitosas deberán de disparar una actualización al perfil que se asocia con las aplicaciones descargadas para un titular de tarjeta en particular, junto con la correcta aplicación del ciclo de vida.

Es importante que el código de esta aplicación y datos para efectuar el proceso de personalización asociados no residan en el ambiente del SGTI del emisor. El código ejecutable de las aplicaciones puede ser importado desde una aplicación de proveedor y almacenarse de manera segura hasta que el proceso de carga sea invocado. Esto también puede ser ejecutado como requerimiento para descargas en postemisión dependiendo de la interfaz de la base de datos de la aplicación y la infraestructura de descarga.

También, el emisor necesitará hacer convenios de negocios con los proveedores de las aplicaciones y proveedores de servicios de tercera parte para direccionar los procedimientos de estos eventos. Los acuerdos de estos servicios pueden incluir entrega segura en línea de aplicaciones y datos para la carga de aplicaciones en el servidor o el emisor puede elegir dar permisos a las solicitudes de aplicaciones viniendo directamente del servidor del proveedor de aplicaciones.

Las descargas pueden ocurrir usando una sesión en línea entre el servidor de carga y la tarjeta directamente o por ensamble de paquetes o scripts, una vez que una sesión de llaves está establecida. Las instrucciones de estos paquetes son sesiones de llaves cifradas de mensajes de código de autenticación (MAC por sus siglas en inglés, Messages Authentication Code) y se envían como una aplicación de descarga.

Un paquete similar puede ser creado para subsecuentes personalizaciones o los paquetes pueden ser combinados. El paquete necesitará ser ubicado en un formato de archivo en particular que sea aceptable por el dispositivo de aceptación de la tarjeta, el cual puede ejecutar el paquete en la tarjeta y regresar los resultados.

Alternativamente los procesos de postemisión podrían tomar lugar como una instrucción-instrucción basada entre la tarjeta, el dispositivo de aceptación de la

tarjeta y el servidor de carga de aplicaciones. Una combinación entre ellos también es factible.

Finalmente, para la terminación del proceso de descarga, se deberá de realizar la notificación de los resultados al emisor de la tarjeta, para esta actividad el ambiente del SGTI es requerido.

El Diccionario EO17 expresa los requerimientos funcionales para la descarga de aplicaciones

Diccionario 24. DO18 Requerimientos del subproceso: Postemisión: Canales de descarga de aplicaciones

Una aplicación descargada puede ser requerida por múltiples fuentes externas y por múltiples entidades empresariales incluyendo al titular de la tarjeta o el proveedor de las aplicaciones. El emisor o proveedor de las aplicaciones pueden también preautorizar una o más aplicaciones específicamente diseñadas para un producto en particular. En este caso, se requiere que una aplicación, sea automáticamente garantizada su conclusión y que el servidor de descarga pueda recuperar el archivo de carga directamente desde una aplicación almacenada de manera segura.

Los requerimientos funcionales para este tema están desarrollados en el diccionario EO18.

El ambiente del SGTI deberá de soportar los mecanismos descritos, incluyendo las interfaces en línea al servidor de carga de aplicaciones, que deberá de alertar de la existencia de una solicitud de descarga.

Si la tarjeta está en línea en el momento de la petición, o cuando la tarjeta está vista en un dispositivo apropiado, el proceso de descarga deberá de dispararse.

Diccionario 25. DO19 Requerimientos del subproceso: Postemisión: Descarga segura de aplicaciones.

Por norma, el ambiente de preemisión debe de ser seguro, se debe conocer y se debe de controlar. El emisor conoce quien está manejando sus tarjetas, que dispositivos están leyendo o escribiendo datos en las tarjetas y que procesos están siendo operados. En resumen el emisor tiene acceso a las tarjetas en cualquier momento para controlar la seguridad o propósitos de control de calidad.

En el ambiente de postemisión, el escenario es completamente diferente. En el peor de los casos posibles, el emisor puede no conocer quien está manejando las tarjetas, que dispositivos las están accesando, que procesos se están realizando o si existe un SGTI que está en comunicación con la tarjeta.

Dependiendo de los requerimientos de seguridad de cada Programa de tarjetas, el ambiente del SGTI, el servidor de descarga de aplicaciones o los dispositivos de descarga seguros pueden generar comandos MAC y cifrarlos en las actividades de postemisión para descargar de manera segura las aplicaciones. Esto requiere acceso a las llaves maestras usadas para derivar las llaves finales del Administrador de la tarjeta o de los dominios de seguridad.

Una vez que la tarjeta ha sido identificada, el servidor de carga seguro deberá recuperar la derivación de datos y derivará las llaves correctas del Administrador de la tarjeta (Card Manager) o dominios de seguridad. Estas llaves en conjunto con una conexión en línea son necesarias para establecer un conjunto de sesiones de llaves. La lista requerida de comandos y sus detalles son definidos en la especificación de tarjeta de GP. En resumen, el registro de titulares, proveedor de aplicaciones e infraestructura de descarga con el ambiente del SGTI pueden aumentar la seguridad de GP.

El Diccionario EO19 expresa los requerimientos funcionales para la descarga segura de aplicaciones

Diccionario 26. DO20 Requerimientos del subproceso: Postemisión: Recuperación de errores en la descarga de aplicaciones

El ambiente de postemisión es mucho menos estable y administrable que el ambiente de preemisión. El proceso puede ser parcialmente controlado por el titular de la tarjeta quien puede tomar acciones impredecibles. Con el fin de asegurar la integridad del Programa de tarjetas, los potenciales problemas necesitan un conjunto de requerimientos adicionales para errores de conexión y recuperación de los mismos.

El diccionario EO20 incluye los requerimientos funcionales para la recuperación de errores de descarga:

A parte de la recuperación del error, escenarios menos administrables pueden manifestarse y requerirán el uso de procesos de postemisión e infraestructura.

En este caso, la recuperación completa de la tarjeta puede ser requerida. También en el evento de pérdida de la tarjeta, robo u otro evento catastrófico, la recuperación de la tarjeta será requerida.

Diccionario 27. DO22 Requerimientos del subproceso: Postemisión: administración delegada

En muchos programas de tarjetas inteligentes con complejas multiaplicaciones, la descarga en postemisión puede ser delegada a proveedores de tercera parte bajo la supervisión del emisor.

Las solicitudes de aplicaciones para descarga usando Administración delegada deberán de tener mecanismos de seguridad tales como tokens generados para el emisor y verificación de blocks de datos patrones de autenticación (DAP) para revisar la integridad. Después de cargar e instalar la aplicación, los datos de la personalización puede ser necesario que sean formateados, actualizados o incrementados.

Ciertos elementos de la personalización de datos pueden ser recuperados desde el titular durante el proceso. Estos requerimientos de personalización pueden tener implicaciones en relación a la interconexión con las bases de datos del titular y preparación de datos para la personalización en tiempo real.

Si la tarjeta soporta administración delegada de tercera parte, el emisor tendrá que informar al proveedor de aplicaciones de los requerimientos para las llaves iníciales del proveedor de aplicaciones. Estas llaves pueden ser obtenidas a través de la llave de transporte, desde el proveedor de aplicaciones y almacenadas en el ambiente del SGTI y SGLL.

Para la administración delegada, los requerimientos funcionales están considerados en el Diccionario EO22.

Diccionario 28. DO23 Requerimientos del subproceso: Postemisión: Procesos de usabilidad del titular de la tarjeta

Si descargas en actividades de postemisión son trabajadas frecuentemente, es muy importante, que los procesos sean tan fáciles de ejecutar como sea posible para el titular de la tarjeta. Diferentes grados de usabilidad pueden ser deseables dependiendo de las limitaciones de las interfaces de usuario y requerimientos de negocio.

Definición de requerimientos funcionales de este proceso están señalados en el diccionario EO23.

Eslabón mercadotecnia y ventas:

Este proceso tiene interfaz con los subprocesos:

DO5: Definición del portafolio
DO6: Compatibilidad del portafolio
DO7: Preparación para la producción

Eslabón de servicio:

Este proceso tiene interfaz con los subprocesos:

DO16 Interfaz con otros sistemas

DO17 Descarga de aplicaciones
DO18 Canales de descarga de aplicaciones
DO19 Descarga segura de aplicaciones
DO20 Recuperación de errores en la descarga de aplicaciones
DO21 Administración delegada
DO23 Usabilidad de la tarjeta

Eslabón Desarrollo tecnológico:

Al margen de las especificaciones funcionales, existen servicios de procesos de planeación, emisión y administración de las tarjetas multiaplicativas, que el ambiente del SGTI debe de contener de manera adicional a la funcionalidad central.

Primero, mientras la funcionalidad central del ambiente del SGTI comparte muchas características con otros sistemas de misión crítica, una organización puede desplegar un ambiente del SGTI empleando capacidades de administración de llaves, ya que las tarjetas inteligentes requieren administración robusta y segura de criptografía y de un sistema gestión de llaves.

Segundo, por la amplitud de las capacidades de las tarjetas y modelos de negocios que se soportan, hay numerosos ambientes de arquitectura que un SGTI puede requerir.

Finalmente, funcionalidades más frecuentes como administración, mantenimiento y arquitectura de sistemas, son elementos importantes en el ambiente del SGTI, que sirven para diferenciarlo de otros ambientes de sistemas.

Diccionario 29. DDT1: Requerimientos del subproceso: Soporte a procesos de negocio: Administración de llaves

La seguridad es sinónimo de tarjetas inteligentes y como tal un sistema de tarjetas inteligentes necesita una interfaz con un sistema de gestión de llaves para gestionar las llaves y las llaves relacionadas con los proveedores de aplicaciones. El SGLL necesitará una interfaz con un módulo de hardware seguro (HSM por sus siglas en ingles Hardware Security Module)

La definición de los requerimientos funcionales de la administración de llaves: Especificación de SGLL y del módulo de hardware seguro (HSM), están referidos en el diccionario EDT1.

Requerimientos del subproceso: Soporte a procesos de negocio: Administración y mantenimiento

En la administración y mantenimiento, hay tres categorías de funcionalidad: Control de acceso, conexión y reporteo.

Diccionario 30. DDT2 Requerimientos del subproceso: Soporte a procesos de negocio: Control de acceso

Como en cualquier sistema de gestión computarizado, la administración de rutinas es requerida. Acceso remoto seguro por el administrador del sistema es esencial si el sistema trabajará en un ambiente distribuido como requerimiento. La capacidad de proporcionar diagnósticos en línea de problemas relativos al chip durante la descarga de aplicaciones u otras actividades.
Mientras estos requerimientos son genéricos para cualquier sistema de gestión robusto, para el caso del SGTI son mencionados para integridad de la especificación.

La definición de los requerimientos funcionales de servicios de acceso está señalada en el Diccionario EDT2

Diccionario 31. DDT3 Requerimientos del subproceso. Soporte a procesos de negocio: Archivo

Como elemento importante de la trazabilidad de la gestión integral del SGTI, los registros de las transacciones, registros de descarga y actualización de aplicaciones deberán de ser contempladas por el ambiente del SGTI.
La definición de los requerimientos funcionales de Archivo está comprendida en el diccionario EDT3.

Diccionario 32. DDT4 Requerimientos del subproceso: Soporte a procesos de negocio: Reportes

En términos generales el SGTI, deberá de disponer de un reportador para construir los reportes que se requieran, de acuerdo a las estructuras de datos definidos y las bases de datos existentes. La definición de requerimientos funcionales está contenida en el diccionario EDT4.

Diccionario 33. DDT5 Requerimientos del subproceso: Soporte a procesos de negocios: Arquitectura del sistema

La Arquitectura del sistema deberá de estar administrado por un sistema de entrega y soporte de servicios que incluya: Administración de la configuración, la Administración de la capacidad y la Administración de riesgos y continuidad del negocio. En el diccionario EDT5 están descritos los requerimientos funcionales.

Diccionario 34. DDT6 Requerimientos del subproceso: Soporte a procesos de negocios: Rendimiento

Como ocurre con cualquier sistema automatizado, rendimiento, capacidad y robustez, son esenciales. Sin embargo, podemos tener problemas en balancear entre rendimiento y aspectos operacionales, por dos razones. Primero, es difícil

medir el rendimiento objetivamente desde las diferentes visiones del Programa de tarjetas.

Segundo, la mayoría de los aspectos necesitan ser puestos en contexto durante su uso, motivo por el cual será un tremendo desafío el ambiente integrado y que sea verificado su cumplimiento en la implementación.

Asociado al rendimiento, es necesario contemplar el cumplimiento de los niveles de servicio acordados con usuarios, clientes y proveedores, así como también los servicios asociados a incidentes y problemas.

Los requerimientos funcionales se expresan en el diccionario EDT6.

Diccionario 35. DDT7 Requerimientos del subproceso: Soporte a procesos de negocio: Interfaces externas

Para interfaces externas, estos requerimientos funcionales deberán ser considerados

En los apartados 3.3, 3.6 y 3.7 de este trabajo se describen los SI con los que el SGTI tiene interacción e interfaces y generan requerimientos a implementar.

La definición de requerimientos de interfaces con sistemas internos y externos, se encuentran expresados en el Diccionario EDT7.

Diccionario 36. DDT8 Requerimientos del subproceso: Soporte a procesos de negocio: Consideraciones de implementación.

Un ambiente de gestión de tarjetas es requerido como interfaz con una variedad de SI relacionados. Estos sistemas pueden incluir aplicaciones de sistemas, infraestructura de dispositivos de aceptación de tarjetas, soporte de sistemas, sistemas de facturación y sistemas de personalización. Es recomendable conocer exactamente que interfaces son requeridas para ciertas implementaciones, para mayor interoperabilidad, es deseable intentar estandarizar estas interfaces donde sea posible.

En los apartados 2.8 y 3.8 se describieron los principales estándares y normas que deben de cumplirse, principalmente para la seguridad y compatibilidad en la conexión y transferencia de datos.

Por la complejidad y naturaleza crítica de muchas de estas interfaces, hay algunos requerimientos adicionales para desplegar en un ambiente de SGTI de gama alta.

La definición de los requerimientos de implementación con interfaces externas se incluye en el diccionario EDT8.

Diccionario 37. DDT9 Requerimientos del subproceso: Soporte a procesos de negocios: Ambiente de la arquitectura

El ambiente de la Arquitectura examina los requerimientos funcionales para diferentes tipos de ambientes de tarjetas inteligentes multiaplicativas. Los siguientes escenarios son examinados:

- Ambiente de SGTI con multiaplicaciones y sitios de almacenamiento de datos
- Capas de tecnología y ambientes de los SGTI distribuidos

Los requerimientos funcionales están señalados en el Diccionario EDT9.

Diccionario 38. DDT10 Requerimientos del subproceso: Soporte a procesos de negocio: Multiaplicaciones y almacenes de datos

La definición de los requerimientos de escenarios donde participan multi aplicaciones y/o sitios de almacenes de datos dictarán requerimientos específicos para preemisión y reemplazo de tarjetas y descarga de aplicaciones en post emisión.

El diccionario EDT10 establece los requerimientos funcionales para este subproceso.

Diccionario 39. DDT11 Requerimientos del subproceso: Soporte a procesos de negocio: Ambientes distribuidos

Para ambientes distribuidos los siguientes requerimientos deberán ser considerados:

- El ambiente del SGTI deberá de soportar la colección de datos, de múltiples de sistemas distribuidos y resultados de la distribución de los subprocesos de personalización y de los resultados del soporte de subsistemas distribuidos

- El ambiente del SGTI deberá soportar procesos de sincronización de datos entre sistemas de gestión de tarjetas distribuidos y de un sistema central

El Diccionario EDT11 describe los requerimientos funcionales de este subproceso.

Diccionario 40. DDT12 Requerimientos derivados del cumplimiento de estándares y normas que aplican

En la mayor parte de los procesos en los que intervienen las tarjetas y el SGTI ocurren intercambio y transferencia de datos. El procesamiento de datos debe de

realizarse cumpliendo los estándares que señalan los diferentes organismos con facultades técnicas y legales.

Estándares de ISO/IEC, ANSI, EMV, NIST, IEEE, EMV deben de ser considerados en el diseño de las aplicaciones del SGTI y en la compatibilidad de la infraestructura que se opere.

En el portafolio del perfil de aplicaciones deben de estar listados aquellos perfiles de plataformas, tarjetas, sistemas operativos que deban de cumplir de acuerdo a requerimiento de conformidad con la seguridad integral como la Evaluación de niveles de seguridad (EAL, Evaluation assurance levels) o Criterios de evaluación de la seguridad de tecnologías de la información (ITSEC, Information technology security evaluation criteria).

En el apartado 2.8 de este trabajo se refirieron los estándares y normas que deben de cumplir las tarjetas, en el apartado 3.8 los que están asociados con el SGTI, SGLLL y HSM.

En el diccionario EDT12 están contenidos los requerimientos funcionales.

Eslabón de Infraestructura organizacional:

Diccionario 41. DIO1: Requerimientos del subproceso. Soporte a procesos de negocios: Soporte a facturación

Dependiendo del modelo de negocios del emisor y acuerdos de negocios con otras entidades empresariales participantes en el Programa, el ambiente del SGTI y aplicaciones relacionadas en el mismo, el ambiente del SGTI y las aplicaciones del servidor de carga pueden tener la capacidad para cobrar por cada actividad, incluyendo la descarga de aplicaciones. Alternativamente, esta funcionalidad puede ser realizada por otro sistema que sea operado por el emisor.

El cargo de un honorario específico puede ser por el titular, proveedor de aplicaciones u otras partes. El sistema podría incluir la opción de renta del estado real de la tarjeta.

Los requerimientos funcionales que pudieran ser implementados están señalados en el diccionario EIO1.

Diccionario 42. DIO2: Requerimientos del subproceso: Sistema de gestión de la calidad

En el diccionario EIO2 están descritos los requerimientos funcionales.

Diccionario 43. DIO3: Requerimientos del subproceso: Sistema de gestión de la seguridad de la información

En el diccionario EIO3 están descritos los requerimientos funcionales.

c) Línea base de la Arquitectura de negocios:

Como entregable de la fase de Visión de la arquitectura y partir de los documentos formales que se dispongan en los que se describan los procesos de negocios se formará la Línea base de la arquitectura de negocios, pudiendo ser los siguientes:

- Acta constitutiva de la empresa
- Manual de organización
- Manual de métodos y procedimientos
- Sistemas de gestión de la calidad
- Sistemas de gestión de la seguridad de la información
- Plan estratégico
- Planes de negocio
- Programas anuales de trabajo
- Normas internas
- Normatividad a la que se sujeta
- Diagnostico de la situación actual de la Arquitectura de negocios

La Línea base de la arquitectura de negocios, se debe de estructurar de acuerdo a los procesos de cadena de valor y de soporte, donde se debe de representar el estado actual que guardan cada uno de los diversos componentes, en términos de poder posteriormente realizar el análisis de brechas entre la situación declarada y la situación que arrojen los requerimientos formulados.

El estado actual que guarda la organización toma el resultado de la planeación estratégica realizada, de acuerdo con Corona [44] y Morrisey [45] plasmada en el análisis FODA (fortalezas, oportunidades, debilidades y amenazas) traduciéndose en los proyectos y procesos a realizar por la organización para alinearse con la Visión definida.

d) Matriz de Responsabilidades RACI

En el apartado 3.3 de este trabajo están referidas las entidades empresariales involucradas en el SGTI, en la tabla DA de ese apartado se enlistan sus roles, esto de acuerdo a varios autores y a la especificación de Global Platform como se referencian en el mencionado apartado.

Partiendo de la estructura organizacional, los roles y responsabilidades de los involucrados en el SGTI, se construye la matriz de responsabilidades RACI (por sus siglas en inglés responsible (responsable), accountable (encargado), consulted (consultado), informed (informado)), la cual presenta de manera estructurada a las personas nombradas por parte de las entidades empresariales involucradas que tienen injerencia directa en el SGTI, en cualquiera de sus etapas.

En el Anexo 2 se presenta la matriz RACI.

e) Arquitectura de negocios

A partir del análisis de brechas entre la Línea base de la Arquitectura de negocios y de los requerimientos formulados se obtiene la primera versión de la Arquitectura de negocios.

Cabe destacar, que el análisis de brechas puede arrojar un rediseño y reingeniería de los procesos de la organización, el cual en su salida debe de proporcionar la nueva estructura de procesos. Para los propósitos de este trabajo, se considera que los procesos documentados corresponden a las iniciativas y visión de la Arquitectura propuesta.

Es oportuno también aclarar en este punto que hay actividades que no están incluidas en el alcance de este trabajo que impactan directamente a la Arquitectura de negocios como es el caso del transporte físico de llaves, el cual en su caso correspondería al dominio de logística de salida, de la ceremonia de llaves que correspondería al dominio de operaciones, así como las actividades de los dominios de mercadotecnia y ventas, adquisiciones y la administración de los recursos humanos.

De acuerdo con Ian Sommerville [9], los requerimientos del sistema pueden ser clasificados en funcionales, no funcionales y de dominio.

Los requerimientos funcionales describen la funcionalidad o servicios que se espera que el sistema proporcione, los requerimientos no funcionales son aquellos que no están directamente ligados con las funciones específicas entregadas por el sistema, ellos pueden relacionar propiedades emergentes al sistema como confiabilidad, tiempos de respuesta y capacidad de las áreas de almacenamiento.

Alternativamente pueden definir restricciones del sistema como son capacidades de los dispositivos de entrada/salida y la representación de datos utilizados en interfaces del sistema.

Los requerimientos de dominio son derivados del área de aplicación del sistema y de las necesidades especificas de los usuarios del mismo, en el caso del SGTI son las especificaciones determinadas por los estándares y normas de ISO/IEC, EMV, ANSI, FIPS, IEEE, principalmente para el tratamiento de las transacciones de intercambio y transferencia de datos entre la tarjeta, el SGTI y sistemas con los que tiene interface, así como la implementación de los algoritmos y niveles de seguridad en el entorno de la operación de la tarjeta inteligente.

De acuerdo a lo anterior los requerimientos formulados para cada eslabón de la cadena de valor y soporte, se pueden presentar de la siguiente forma:

Diccionario	Descripción del requerimiento	Eslabón al que pertenece	Interfaz con eslabón	Tipo de requerimiento
DL1	Administración del inventario de tarjetas	Logística de entrada		Funcional
DO3	Definición y registro de la tarjeta	Operaciones		Funcional
DO4	Definición y registro de aplicaciones	Operaciones		Funcional
DO5	Definición del portafolio	Operaciones	Mercadotecnia y ventas	Funcional
DO6	Compatibilidad con el portafolio	Operaciones	Mercadotecnia y ventas	Funcional
DO7	Preparación para la emisión	Operaciones	Mercadotecnia y ventas	Funcional
DO9	Habilitación de la tarjeta	Operaciones		Funcional
DO10	Preparación de datos, personalización	Operaciones		Funcional
DO11	Post personalización	Operaciones	Logística de salida	Funcional
DO12	Terminación de la producción	Operaciones	Logística de salida Mercadotecnia y ventas	Funcional
DO14	Gestión de vida de las tarjetas	Operaciones		Funcional
DO15	Gestión de vida de las aplicaciones	Operaciones		Funcional
DO16	Interfaz con otros sistemas	Operaciones	Servicio	No funcional
DO17	Descarga de aplicaciones	Operaciones	Servicio	Funcional
DO18	Canales de descarga de aplicaciones	Operaciones	Servicio	Funcional
DO19	Descarga segura de aplicaciones	Operaciones	Servicio	Funcional
DO20	Recuperación de errores en la descarga de aplicaciones	Operaciones	Servicio	Funcional
DO22	Administración delegada	Operaciones		No funcional
DO23	Usabilidad de la tarjeta	Operaciones	Servicio	No funcional
DDT1	Administración de llaves	Desarrollo tecnológico		Funcional
DDT2	Control de acceso	Desarrollo tecnológico		Funcional
DDT3	Archivo	Desarrollo tecnológico		Funcional
DDT4	Reportes	Desarrollo		Funcional

Diccionario	Descripción del requerimiento	Eslabón al que pertenece	Interfaz con eslabón	Tipo de requerimiento
		tecnológico		
DDT5	Arquitectura del sistema	Desarrollo tecnológico		No funcional
DDT6	Rendimiento	Desarrollo tecnológico		No funcional
DDT7	Interfaces externas	Desarrollo tecnológico		No funcional
DDT8	Consideraciones de la Implementación	Desarrollo tecnológico		No funcional
DDT9	Ambiente de arquitectura	Desarrollo tecnológico		No funcional
DDT10	Multiaplicaciones y almacén de datos	Desarrollo tecnológico		No funcional
DDT11	Ambientes distribuidos	Desarrollo tecnológico		No funcional
DDT12	Estándares y normas	Desarrollo tecnológico		Dominio
DIO1	Soporte a facturación	Infraestructura organizacional		Funcional
DI02	Gestión de la calidad	Infraestructura organizacional		No funcional
DI03	Gestión de la seguridad de la información	Infraestructura organizacional		No funcional

La figura 53 muestra una representación de la Arquitectura de negocios, mapeada a partir de los diccionarios que describen los requerimientos del SGTI y la tabla 32 los enlista de acuerdo al eslabón que les corresponde.

Tabla 32. Arquitectura de negocios, representada por sus cadenas de valor y soporte

Arquitectura de negocios

Cadena de valor				
Logística de entrada	**Operaciones**	**Logística de salida**	**Mercadotecnia y ventas**	**Servicio**
DL1	DO3 DO4 DO5 DO6 DO7 DO9 DO10 DO11 DO12 DO13 DO14 DO15			

Cadena de valor				
Logística de entrada	**Operaciones**	**Logística de salida**	**Mercadotecnia y ventas**	**Servicio**
	DO16 DO17 DO18 DO19 DO20 DO22 DO23			

Cadena de soporte			
Adquisiciones	**Desarrollo tecnológico**	**Administración de recursos humanos**	**Infraestructura organizacional**
	DDT1 DDT2 DDT3 DDT4 DDT5 DDT6 DDT7 DDT8 DDT9 DDT10 DDT11 DDT12		DIO1 DIO2 DIO3

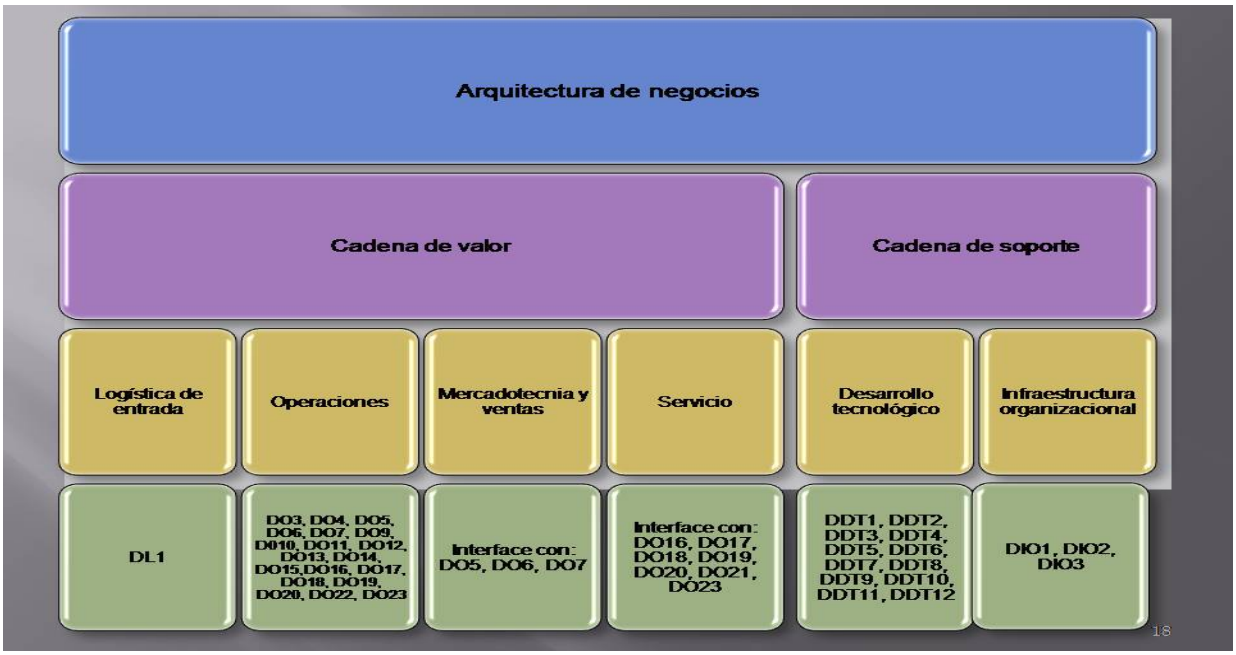


Figura 53. Representación de la arquitectura de negocios, mediante sus cadenas de valor y soporte

Fase C: Arquitectura de información

De acuerdo con TOGAF, la Arquitectura de información está conformada por la Arquitectura de las aplicaciones y la Arquitectura de los datos.

Arquitectura de aplicaciones

El SGTI es un conjunto de aplicaciones diseñadas arquitectónicamente a través de las herramientas que proporciona la Ingeniería del software, en su más amplia gama, desde los métodos hasta las herramientas tecnológicas.

De acuerdo con Pressman [3], la Arquitectura de software en su forma más simple, es la estructura u organización de los componentes del programa (módulos), la manera en que estos componentes interactúan, y la estructura de datos que utilizan los componentes.

Como lo menciona Pressman [3], Brad Appleton establece que

> "un patrón de diseño describe una estructura de diseño que resuelve un problema de diseño en particular dentro de un contexto especifico y en medio de fuerzas que pueden tener impacto en la manera en que se aplica y utiliza el patrón".

A la luz de lo anterior, se establece que los patrones de arquitectura y diseño del software materializan la modularidad, es decir las aplicaciones (el software) se dividen en componentes que es posible abordar de manera individual.

De los diversos modelos de representación arquitectónica, entre otros, existen los denominados modelos funcionales que se utilizan para representar la jerarquía funcional de un sistema. Para los propósitos de este trabajo de tesis seleccionamos este modelo para representar la arquitectura de las aplicaciones.

a) Diccionarios de especificaciones funcionales

Los requerimientos funcionales corresponden al mapeo de los requerimientos de negocio hacia las reglas funcionales. De acuerdo a los directorios de requerimientos obtenidos en la fase de arquitectura de negocio, el mapeo correspondiente lo obtenemos en los diccionarios de especificaciones o requerimientos funcionales.

Donde f (h), es la explosión a niveles más a detalle e identificando para el ambiente del SGTI, si las funciones son realizadas de manera automatizada y/o manualmente.

DRi --→-f (h)---→ DFi, donde DRi es el diccionario de requerimientos de negocios y DFi es el diccionario funcional.

El ambiente del SGTI incluye las funcionalidades que son automatizadas y las no automatizadas, las cuales se definen en los siguientes diccionarios de especificaciones funcionales, para el caso de que apliquen estas últimas se relacionan como "Funcionalidad no automatizada".

De acuerdo con las publicaciones de Global Platform [R28], [R29] y [R30], implementaciones realizadas en gobiernos [R24], [R25] y [R26] y recomendaciones del GSA (General Services Administration) de Estados Unidos las especificaciones a detalle que corresponden a los requerimientos de procesos de negocios los podemos relacionar mediante los siguientes diccionarios de especificaciones.

Diccionario 44.EL1: Diccionario especificación funcional del subproceso: Soporte a procesos de negocios: Administración del inventario de tarjetas

Ref.	Funcionalidad
EL1.1	Dar seguimiento a la distribución de tarjetas y a los dispositivos asociados de aceptación de las mismas.
EL1.2	Administrar los inventarios de tarjetas
EL1.3	Procesar los puntos críticos de los inventarios

Diccionario 45. EO3 Especificación funcional del subproceso: Definición y registro de la tarjeta

Ref.	Funcionalidad
EO3.1	Registrar y administrar los perfiles de tarjetas, a partir de los parámetros que lo componen
EO3.2	Importar y exportar perfiles de tarjetas, desde proveedores hacia emisores, en concordancia con los perfiles registrados
EO3.3	Administrar múltiples perfiles de tarjetas
EO3.4	Disponer de un módulo de acceso seguro, con permisos y privilegios tanto a entidades internas y externas.
EO3.5	Ser interfaz con el sistema operativo de la tarjeta para el registro histórico de los diferentes estados del ciclo de vida que vaya ocurriendo
EO3.6	Almacenar y administrar los requerimientos externos de la tarjeta y cualquier dependencia asociada a las aplicaciones
EO3.7	Dar seguimiento al dominio de seguridad de la tarjeta, al propietario de cada dominio de seguridad y a los privilegios de cada dominio de seguridad
EO3.8	Administrar tarjetas a través de diferentes versiones de perfiles y de plataformas

Diccionario 46. EO4 Especificación funcional del subproceso: Definición y registro de aplicaciones

Ref.	Funcionalidad
EO4.1	Registrar y administrar los perfiles de las aplicaciones a partir de los parámetros que las componen
EO4.1	Importar y exportar perfiles de aplicaciones en concordancia con la especificación de perfiles
EO4.2	Almacenar y administrar la fecha de expiración de los requerimientos de la aplicación
EO4.3	Asociar un archivo de carga de una aplicación particular con un rango de tarjetas compatibles desde la base de datos del perfil de aplicaciones
EO4.4	Administrar el registro de aplicaciones válidas, con o sin una autoridad certificadora
EO4.5	Almacenar y administrar los requerimientos de las aplicaciones para inicialización, incluyendo parámetros de carga e inicialización
EO4.6	Ser capaz de soportar DAP (Patrones de datos de autenticación), usando internamente o externamente DAP generados, para asegurar la integridad de los datos de archivos de carga
EO4.7	Captar los objetos compartidos e información de dependencia de applets, para soportar desarrollos futuros en operaciones de descarga postemisión
EO4.8	Dar mantenimiento a los requerimientos actualizados de la aplicación, preemisión y postemisión, de tal forma que la aplicación pueda ser cargada e instalada en postemisión
EO4.9	Almacenar y administrar la carga de archivos de perfiles y archivos asociados de carga basados en referencias proporcionadas en los datos del perfil de la aplicación
EO4.10	Almacenar y administrar la ubicación del código ejecutable de la aplicación o archivos de carga desde las aplicaciones de los proveedores o desarrolladores, los cuales son usados como una entrada de los procesos de carga de la aplicación

Diccionario 47. EO5 Especificación funcional del subproceso: Definición del portafolio

Ref.	Funcionalidad
EO5.1	Permitir a usuarios seleccionar una tarjeta desde el perfil de tarjetas.
EO5.2	Permitir a un emisor seleccionar una lista de aplicaciones requeridas u opcionales a ser asociadas con la tarjeta como un portafolio primario de aplicaciones
EO5.3	Permitir al emisor seleccionar una lista de aplicaciones que pueden ser descargadas en postemisión en la tarjeta

Ref.	Funcionalidad
EO5.4	Permitir a un emisor seleccionar una lista de perfiles de aplicaciones y que el SGTI calcule un perfil de tarjeta
EO5.5	Calcular el ROM, RAM, EEPROM y requerimientos criptográficos para presentar a un fabricante de tarjetas para la selección del circuito integrado y el desarrollo de la máscara apropiada
EO5.6	Asociar el portafolio con una o más definiciones de tarjeta (perfiles) considerando definiciones adicionales de la tarjeta que estén disponibles
EO5.7	Proporcionar las facilidades para el gobierno de la dependencia entre el ciclo de vida de las diferentes aplicaciones de la tarjeta
EO5.8	Ejecutar los controles de compatibilidad en términos de las reglas de negocios entre la tarjeta y las aplicaciones, basadas en la información de las definiciones de tarjeta y aplicaciones
EO5.9	Ejecutar los controles de compatibilidad en términos de las reglas técnicas entre las aplicaciones del chip y las capacidades del chip, basadas en la información proporcionada en los perfiles de la aplicación y definiciones de la tarjeta
EO5.10	Alertar de conflictos de negocios entre la mezcla de aplicaciones y la tarjeta elegida
EO5.11	Alertar de conflictos técnicos entre la mezcla de aplicaciones y la tarjeta elegida
EO5.12	Asegurar la compatibilidad de las aplicaciones en términos de posibles interacciones, conflictos de marca, actualización de llaves iníciales y definición de aplicaciones

Diccionario 48. EO6 Especificación funcional del subproceso: Compatibilidad del portafolio

Ref.	Funcionalidad
EO6.1	Controlar el ambiente de ejecución y versión para compatibilidad con las aplicaciones que son cargadas
EO6.2	Controlar la compatibilidad de la versión de la plataforma
EO6.3	Controlar la memoria persistente mutable (EEPROM), requerimientos de espacio para código y datos para nuevas aplicaciones que se requieran estar dispuestas en la tarjeta
EO6.4	Evitar supresiones o borrar pistas de aplicaciones que fueron borradas, especialmente en tarjetas inteligentes con limitaciones tecnológicas que no garantizan memoria contigua suficiente en EEPROM
EO6.5	Controlar los requerimientos de RAM para nuevas aplicaciones que estén disponibles en el perfil de la tarjeta actual
EO6.6	Controlar los requerimientos criptográficos de las aplicaciones que puedan ser incorporadas a la tarjeta

Diccionario 49. EO7 Especificación funcional del subproceso: Preparación para la emisión

Ref.	Funcionalidad
EO7.1	Ser interfaz con el SGLL para generar de manera segura una llave para cifrar las llaves necesarias para la protección durante el transporte de las llaves maestras del proveedor u otras llaves de aplicaciones del proveedor.
EO7.2	Recibir y almacenar la información del fabricante del CI como el número de serie de la tarjeta para: • Prepersonalizar el CI • Prepersonalizar la fecha del CI • Identificar el equipo de pre personalización del CI
EO7.3	Importar o actualizar la información del perfil de la tarjeta, basada en información del fabricante del CI y del conjunto de aplicaciones asociadas a la máscara
EO7.4	Mantener los estados del ciclo de vida de las aplicaciones de la máscara, basadas en información del fabricante
EO7.5	Ser interfaz con el SGLL para derivar de manera segura una llave inicial maestra de proveedor y cifrarla para su transporte al fabricante del circuito integrado
EO7.6	Proveer código de aplicaciones o archivos de carga requeridos por el proveedor del circuito integrado para el proceso de enmascaramiento.

Diccionario 50. EO8 Especificación funcional del proceso de producción

Proceso: Producción	Subprocesos
	Habilitación de la tarjeta
	Personalización de la tarjeta
	Emisión de la tarjeta

Diccionario 51. EO9 Especificación funcional del subproceso: Habilitación de la tarjeta

Ref.	Funcionalidad
EO9.1	Tener interfaz con el SGLL para la generación y derivación de las llaves
EO9.2	Tener interfaz con el SGLL para la generación y cifrado de las llaves de transporte de las tarjetas al habilitador o fabricante de la tarjeta
EO9.3	Almacenar los resultados de la habilitación, el estado del ciclo de vida de la tarjeta y el estado del ciclo de vida de las aplicaciones cargadas por el fabricante
EO9.4	Actualizar el perfil individual de la tarjeta basado en la información del fabricante proporcionada por los diversos vendedores, para reflejar el

Ref.	Funcionalidad
	estado del ciclo de vida de la tarjeta INITIALIZED
EO9.5	El SGTI o el SGLL relacionado pueden generar las llaves derivadas finales del emisor desde la llave maestra final del emisor. Este requerimiento específicamente aplica al caso donde la personalización ocurre con un despacho
EO9.6	Incorporar componentes del lenguaje interprete de scripts para crear el conjunto de instrucciones o scripts para cargar e instalar los dominios de seguridad e inicializar el Administrador de la tarjeta
EO9.7	Crear las instrucciones o scripts para instalar los Dominios de seguridad sobre el "área" del proveedor de aplicaciones y personalizar el dominio de seguridad con las llaves proporcionadas para las aplicaciones
EO9.8	Registrar los datos asociados al ciclo de vida de la tarjeta. Estos datos incluyen: • Prepersonalización del CI • Fecha de prepersonalización del CI • Identificador del equipamiento de la pre personalización del CI

Diccionario 52. EO10 Especificación funcional del subproceso: Preparación de datos/personalización

Ref.	Funcionalidad
EO10.1	Generar un número de referencia (CRN) para ser asociado con un titular de la tarjeta y compartir como un número lógico de referencia común entre aplicaciones de proveedores y sistemas relacionados
EO10.2	Generar un número único por tarjeta, el cual identificará la tarjeta y será asociado con el CRN. Este el número de imagen de la tarjeta (CIN). El CIN es escrito en la tarjeta durante la personalización y puede opcionalmente ser asociado con el CRN
EO10.3	Ser interfaz con el SGLL para generar y almacenar de manera segura la llave maestra final del Administrador de la tarjeta (Card Manager), usada para derivar las llaves finales del Administrador de la tarjeta
EO10.4	Ser interfaz para la generación de las llaves derivadas finales del Administrador de la tarjeta y opcionalmente las llaves derivadas del dominio de seguridad usando el CIN como dato derivado
EO10.5	Generar un archivo de datos personalizados cotejados, basado en el CRN , las entradas desde varios sistemas de aplicaciones y requerimientos de personalización para cada aplicación
EO10.6	Distribuir de manera segura el archivo de scripts de personalización para el despacho o sistema de personalización
EO10.7	Actualizar el producto, en su base de datos y sistemas de información del proveedor de las aplicaciones que resulten del proceso de personalización
EO10.8	El SGTI o componentes del intérprete de lenguaje de scripts debe de

Ref.	Funcionalidad
	preparar un conjunto de scripts de personalización basados en la tarjeta e información del perfil de las aplicaciones
EO10.9	Crear un producto específico de tarjeta por grupo de titulares de tarjeta basados en una suite predeterminada de aplicaciones o datos estáticos de las aplicaciones

Diccionario 53. EO11 Especificación funcional del subproceso: Postpersonalización

Ref.	Funcionalidad
EO11.1	Actualizar los datos asociados al estado del ciclo de vida “SECURED”
EO11.2	Actualizar el estado del ciclo de vida para las aplicaciones de la tarjeta desde los estados de “SELECTABLE” a “PERSONALIZED” según la plataforma seleccionada
EO11.3	Actualizar las aplicaciones de los sistemas relevantes con los resultados de los procesos de personalización pertinentes para cada aplicación
EO11.4	Almacenar la información pertinente a la producción: • Personalización del CI • Fecha de personalización del CI • Identificadores del equipamiento de personalización del CI

Diccionario 54. EO12 Especificación funcional del subproceso: Terminación de la producción

Ref.	Funcionalidad
EO12.1	Proveer actualizaciones a las aplicaciones del sistema del emisor o aplicaciones del sistema del proveedor con las solicitudes de aplicaciones de personalización
EO12.2	Recuperar el perfil ID o datos del titular del titular de la tarjeta en consultas a partir del CRN o CIN

Diccionario 55. EO1 Especificación de los procesos de postproducción

Proceso: Postproducción	Subprocesos
	Gestión del ciclo de vida de la tarjeta
	Aplicación del ciclo de vida de la tarjeta
	Postemisión
	Soporte a procesos de negocio

Diccionario 56. EO14 Especificación funcional del subproceso: Gestión del ciclo de vida de la tarjeta

Ref.	Funcionalidad
EO14.1	Registrar, administrar y dar seguimiento a cualquier cambio del estado del ciclo de vida de la tarjeta
EO14.2	Dar seguimiento y actualizar el inventario de tarjetas e implementar control de versiones de tarjetas
EO14.3	Dar seguimiento y actualizar el inventario de la plataforma (Java Card, Multos, GP) e implementar el control de cambios de plataforma
EO14.4	Asociar el CRN con una nueva tarjeta para propósitos de reposición en postemisión. Esto puede ser hecho por reencadenamiento del CRN con el CIN en la tarjeta nueva. El CRN es una referencia única lógica hacia el titular de la tarjeta y el portafolio de aplicaciones.
EO14.5	Asociar una nueva tarjeta con un producto existente para propósitos de reemisión
EO14.6	Asociar una nueva tarjeta con un estado existente de ciclo de vida de una tarjeta ya existente
EO14.7	Generar y transmitir las instrucciones para bloquear o terminar una tarjeta
EO14.8	Recibir una notificación de bloquear/terminar una tarjeta y actualizar el estado del ciclo de vida que corresponda.
EO14.9	Establecer los archivos maestros del titular de la tarjeta que contengan la información relevante del titular de la tarjeta y el número de referencia lógico (CRN) o ser interfaz con un archivo maestro del titular de la tarjeta o del sistema de información del cliente

Diccionario 57. EO15 Especificación funcional del subproceso: Gestión del ciclo de vida de las aplicaciones

Ref.	Funcionalidad
EO15.1	Dar seguimiento a los estados del ciclo de vida de las aplicaciones a través de la vida de la tarjeta
EO15.2	Dar seguimiento y actualizar el inventario de aplicaciones e implementar control de versiones de aplicaciones
EO15.3	Administrar cualquier cambio en los perfiles asociados con nuevas versiones de aplicaciones
EO15.4	Asociar a una nueva tarjeta el estado del ciclo de vida de las aplicaciones de una tarjeta existente
EO15.5	Generar y transmitir las instrucciones para bloquear una aplicación
EO15.6	Recibir notificaciones de bloquear/desbloquear aplicaciones y actualizar el correspondiente estado del ciclo de vida de las aplicaciones
EO15.7	Identificar y administrar las aplicaciones, sus correspondientes estados del ciclo de vida, que fueron cargadas en la tarjeta original o en

Ref.	Funcionalidad
	actividades postemisión

Diccionario 58. EO16 Especificación funcional de requerimientos de interfaz con otros sistemas

Ref.	Funcionalidad
EO16.1	Permitir al emisor bloquear completamente una tarjeta, bloquear completamente una aplicación o terminar una tarjeta para prevenir posteriormente actividades fraudulentas o mal funcionamiento de la tarjeta o las aplicaciones
EO16.2	Informar a las aplicaciones del sistema de cualquier solicitud de cambio en el estado de la tarjeta o aplicaciones y recibir los cambios de estado de la tarjeta o de las aplicaciones
EO16.3	Ser interfaz con los servicios al cliente para notificaciones de robo o extravió
EO16.4	Señalar que la tarjeta y las aplicaciones asociadas pueden ser bloqueadas o desbloqueadas en la siguiente actualización en línea
EO16.5	Cumplir las reglas y políticas de negocio, los estados del ciclo de la aplicación deberán de ser alterados en situaciones de robo o extravió
EO16.6	Dar seguimiento al ciclo de vida de tarjetas robadas o extraviadas que deberán de ser reemplazadas hasta que el sistema pueda reportar o confirmar que la tarjeta ha sido destruida.
EO16.7	Soportar el reemplazo de tarjetas emergentes por un periodo de tiempo especificado
EO16.8	Ser interfaz con el sistema de servicio al cliente para notificaciones de reemplazo de tarjetas
EO16.9	Describir el contenido de la tarjeta original, así como subsecuentes descargas que hayan alterado su contenido desde la base de inventario de tarjetas y aplicaciones
EO16.10	Si una tarjeta parcialmente reemplazada es emitida, el ambiente del SGTI deberá de actualizar la base de datos de la tarjeta con las nuevas aplicaciones cargadas en postemisión desde la base de datos del inventario de aplicaciones. Una tarjeta parcialmente reemplazada es definida como una que no tiene el conjunto completo de aplicaciones que estaban presentes en la tarjeta original.

Diccionario 59. EO17 Especificación funcional del subproceso: Postemisión: Descarga de aplicaciones

Ref.	Funcionalidad
EO17.1	Registrar, actualizar y mantener un conjunto de aplicaciones disponibles por producto
EO17.2	Soportar archivos de carga de aplicaciones, colección, empaquetamiento y distribución del servidor de descarga o

Ref.	Funcionalidad
	infraestructura de descarga
EO17.3	Ofrecer soporte para múltiples infraestructuras de descarga (ATM, kioscos, internet, etc.). Esto puede requerir estandarizar las interfaces y requerir elementos de datos entre el ambiente del SGTI y cualquier servidor del sistema de descarga de aplicaciones
EO17.4	Soportar la descarga en postemisión de múltiples proveedores. Esto puede requerir estandarizar las interfaces y requerir elementos de datos entre el ambiente del SGTI y las aplicaciones de los sistemas proporcionados
EO17.5	Ser interfaz con una variedad de dispositivos de aceptación de tarjeta, incluyendo clientes de internet
EO17.6	Operar con ventanas de tiempo razonables para conexión de redes con baja velocidad
EO17.7	Balancear las múltiples solicitudes en línea para descargar aplicaciones
EO17.8	Ser interfaz con el sistema de aplicaciones para recuperar archivos de carga de aplicaciones
EO17.9	Ser interfaz con el sistema de aplicaciones para verificación o validación de datos de personalización
EO17.10	Proporcionar un script o mecanismo similar para paquetes de archivos de carga, instrucciones de carga y cualquier dato relacionado con la personalización, bajo sesiones de llaves cifradas
EO17.11	Transmitir los paquetes/script de los dispositivos de aceptación de tarjetas en una instrucción individual o en base a comandos bajo sesión de llaves
EO17.12	Recibir los resultados exitosos/fallidos de la interacción de tarjetas en los procesos de descarga en post emisión
EO17.13	El servidor de descarga actualizará el ambiente del SGTI relacionado con los resultados del proceso de descarga
EO17.14	Actualizar el perfil del producto de una tarjeta en particular con la información del ciclo de vida de la nueva aplicación
EO17.15	Actualizar las aplicaciones de los sistemas relevantes con los resultados de la descarga de aplicaciones
EO17.16	Almacenar los archivos apropiados de carga de las solicitudes de descarga

Diccionario 60. EO18 Especificación funcional del subproceso: Postemisión: Canales de descarga de aplicaciones

Ref.	Funcionalidad
EO18.1	Actualizar una tarjeta vía una transacción en línea o por requerimiento telefónico de los titulares de las tarjetas
EO18.2	Ser interfaz con el centro de servicio al cliente o sistema de soporte a los titulares para requerimientos de actualización de tarjetas

Ref.	Funcionalidad
EO18.3	Actualizar vía una bandera operada por el SGTI o una petición en línea o telefónica desde el proveedor de aplicaciones
EO18.4	Actualizar la tarjeta directamente en línea utilizando internet, desde el proveedor de la aplicación o sitio web del emisor
EO18.5	Atender de manera directa requerimientos vía teléfonos móviles u otros dispositivos de los consumidores
EO18.6	Permitir al emisor a forzar pro activamente una descarga de tarjetas o grupo de tarjetas

Diccionario 61. EO19 Especificación funcional del subproceso: Postemisión: Descarga segura de aplicaciones

Ref.	Funcionalidad
EO19.1	Proveer los recursos para el registro de todos los usuarios de la infraestructura de descarga
EO19.2	Registrar todos los componentes usados en la infraestructura de descarga
EO19.3	Tener acceso seguro a las llaves maestras del emisor por el ambiente del SGTI o del servidor de descarga a través del SGLL
EO19.4	Establecer la sesión de llaves por parte del servidor de descarga, usando el protocolo de canal seguro con el Administrador de la tarjeta o el dominio de seguridad y llaves derivadas
EO19.5	Asegurar que el estado de la tarjeta es SECURE, y controlar cualquier estado apropiado de la aplicación antes de realizar la descarga en postemisión
EO19.6	El servidor de descarga tendrá que identificar la tarjeta, el emisor, y/o proveedor de aplicaciones para recuperar información acerca de la tarjeta, el emisor o las aplicaciones
EO19.7	Checar que el conjunto de reglas de negocio incluyendo cualquier información que expire apropiadamente antes de realizar la descarga post emisión
EO19.8	Producir archivos de pistas auditoría de las actividades de descarga tales como acceso de los titulares de tarjetas, dispositivos de identificación de clientes y actividades de conexión del sistema
EO19.9	Ofrecer soporte para asegurar la integridad de la transmisión de datos
EO19.10	Asegurar el soporte del protocolo del canal seguro. El servidor de descarga deberá recuperar los datos derivados desde la tarjeta y derivar los apropiados al Administrador de la tarjeta o llaves del dominio de seguridad para establecer la comunicación segura con la tarjeta
EO19.11	Registrar dispositivos de descarga, aprobados por el emisor
EO19.12	Bloquear la tarjeta si la imagen de la tarjeta no corresponde con la imagen del servidor principal

Diccionario 62. EO20 Especificación funcional del subproceso: Postemisión: Recuperación de errores en la descarga de aplicaciones

Ref.	Funcionalidad
EO20.1	Mantener el estatus de cada descarga fallida, por parte del SGTI o del servidor de descarga
EO20.2	Administrar procedimientos para la recuperación de errores en el caso de una descarga parcial o procesos de descarga incompletos, por parte del servidor de descarga
EO20.3	Administrar un conjunto de reglas de negocios para descargas incompletas o parciales, esto puede incluir envió de notificaciones a titulares para tomar una acción posterior por parte del ambiente del SGTI o del servidor de descarga
EO20.4	Determinar los estados de la tarjeta y aplicaciones después de que la descarga está completada por parte del servidor de descarga
EO20.5	Producir archivos de registros de las actividades de descarga por cada error de conexión, producción de registros y registros de la administración del sistema por parte del ambiente del SGTI

Diccionario 63. EO21 Especificación funcional del subproceso: Postemisión: Reemisón de tarjetas

Ref.	Funcionalidad
EO21.1	Soportar remplazos de tarjeta de emergencia o parciales y reemitir hasta que datos suficientes sean garantizados para habilitar una completa reinstalación de las aplicaciones
EO21.2	Reinstalar el conjunto de aplicaciones, incluyendo la administración de cualquier sistema de personalización de datos y/o los valores con las reglas de negocio apropiadas, políticas y parámetros asociados con cada aplicación

Diccionario 64. EO22 Especificación funcional del subproceso: Postemisión: Administración delegada

Ref.	Funcionalidad
EO22.1	Soportar múltiples servicios de proveedores y administración delegada, el ambiente del SGTI /SGLL deberá de generar los tokens para carga e instalación
EO22.2	Mantener los registros para los tokens de carga e instalación que son creados para la tarjeta, y los asociados al proveedor de aplicaciones para quien fueron creados
EO22.3	Permitir la distribución local de los tokens de carga e instalación
EO22.4	Ser interfaz con el SGLL para generar los tokens de carga e instalación basados en la llave privada del emisor y hash del archivo de carga, cuando la administración delegada es soportada

Ref.	Funcionalidad
EO22.5	Mantener los registros de las cargas, instalación y borrado usando recibos de carga, instalación y borrados regresados a través de las actividades de postemisión
EO22.6	Operar información de conformidad de descargas exitosas y fallidas tanto en modo local como en línea

Diccionario 65. EO23 Especificación funcional del subproceso: Postemisión: Procesos de usabilidad para el titular de la tarjeta

Ref.	Funcionalidad
EO23.1	El ambiente del SGTI o servidor de descarga deberán minimizar el nivel de interacción del titular
EO23.2	La infraestructura de descarga deberá de bloquear la tarjeta en sitio (si es posible) durante el proceso de descarga.
EO23.3	El ambiente del SGTI o el servidor de descarga deberán de avisar al usuario específicamente en un lenguaje amigable que no sea técnico cuando sea necesario
EO23.4	La interfaz con el usuario no deberá de desplegar opciones inapropiadas para los usuarios de las tarjetas
EO23.5	El ambiente del SGTI o el servidor de descarga deberán de informar al usuario del tiempo involucrado en cada paso del proceso
EO23.6	El ambiente del SGTI deberá de informar al usuario de los procesos exitosos y fallidos
EO23.7	Informar al usuario de acciones posteriores a tomar en caso de descargas fallidas

Diccionario 66. EDT1 Especificación funcional del subproceso: Soporte a procesos de negocio: Administración de llaves

Ref.	Funcionalidad
EDT1.1	Generar, mantener y distribuir las llaves que se requieran para el transporte seguro, instalación y acceso de las aplicaciones en la tarjeta, por parte del ambiente del SGTI/SGLL
EDT1.2	Generar, mantener y distribuir las llaves que se requieran para la habilitación y personalización de tarjetas y aplicaciones definidas en los requerimientos funcionales del SGLL, por parte del ambiente del SGTI/SGLL
EDT1.3	Ejecutar cálculos criptográficos
EDT1.4	Proporcionar la interfaz para la recepción y distribución de certificados de llave pública desde autoridades certificadoras para soportar especificaciones funcionales del SGLL

Diccionario 67. EDT2 Especificación funcional del subproceso: Soporte a procesos de negocio: Control de acceso

Ref.	Funcionalidad
EDT2.1	Permitir procesos de registro seguro
EDT2.2	Alertar de problemas en el sistema
EDT2.3	Registrar errores y notificar errores severos al administrador del sistema
EDT2.4	Soportar niveles de acceso seguro dependiendo del perfil del usuario
EDT2.5	Proporcionar un sistema de respaldo y recuperación

Diccionario 68. EDT3 Especificación funcional del sub proceso: Soporte a procesos de negocio: Archivo

Ref.	Funcionalidad
EDT3.1	Mantener las pistas de auditorías en línea de las actividades de acceso para cumplir los requerimientos regulatorios
EDT3.2	Proporcionar facilidades para archivar transacciones fuera de línea por varios años para cumplir los requisitos regulatorios

Diccionario 69. EDT4 Reportes

De acuerdo a los requerimientos de la Línea base de la Arquitectura tecnológica, en el apartado de software especial se debe de incluir un servidor de reportes.

Diccionario 70. EDT5 Arquitectura del sistema

Requerimientos que son obtenidos a partir de la Línea base de la Arquitectura tecnológica.

Diccionario 71. EDT Especificación funcional del subproceso: Proceso soporte a proceso de negocios: Rendimiento

Diseñar los servicios de tecnología de la información según ITIL[W14], a partir de la Administración de los niveles de servicios acordados, administración del riesgo, la administración de la demanda, la administración de la capacidad, la administración de la continuidad, la administración de la disponibilidad y la administración de la seguridad.

Ref.	Funcionalidad
EDT6.1	Tener la capacidad para procesar tarjetas relacionadas con transacciones de datos, con exceso de capacidad para los periodos de transacciones pico
EDT6.2	De acuerdo a la plataforma seleccionada y con base en la información histórica de movimientos, transacciones, estimar la capacidad de la infraestructura tecnológica, tomando en cuenta la prospectiva de negocios

Ref.	Funcionalidad
EDT6.3	Diseñar la Arquitectura de seguridad de acuerdo a la administración de riesgos

Diccionario 72. EDT7 Especificación funcional del subproceso: Soporte a procesos de negocio: Interfaces externas

Ref.	Funcionalidad
EDT7.1	Soportar interfaces estándar y protocolos para sistemas externos y empresariales donde sean aplicables., como: • Despachos de personalización • Proveedores de aplicaciones • Sistemas para la preparación de la personalización • Centros de llamadas • Centros de servicios a clientes • Dispositivos de aceptación de tarjetas y servidores de descarga
EDT7.2	Soportar comunicaciones seguras y transmisión de información de acuerdo a la Arquitectura de seguridad
EDT7.3	Manejar accesos generales de datos por sistemas externos, alineados a la Arquitectura de seguridad autorizada
EDT7.4	Usando el CRN como primer identificador, el ambiente del SGTI deberá tener interfaces con otros sistemas para reemisión de tarjetas, con sistemas principales para bloquear aplicaciones por pérdidas y robos, con aplicaciones de sistemas transaccionales y sistemas de proveedores de aplicaciones, de acuerdo a la Arquitectura de seguridad.
EDT7.5	Reportar discrepancias o fallas de las comunicaciones entre sistemas principales, aplicaciones de sistemas y aplicaciones de proveedores de sistemas. De acuerdo al nivel de servicios acordado interna y externamente y de la administración de incidencias y problemas
EDT7.6	Proveer un sistema de soporte al cliente para problemas relacionados con tarjetas o aplicaciones, o interfaces con un sistema ya existente
EDT7.7	Sincronizar los inventarios de tarjetas y aplicaciones con otras bases de datos con información de los titulares, usando el CRN como referencia

Diccionario 73. EDT8 Especificación funcional del subproceso: Soporte a procesos de negocio: Consideraciones de implementación

Ref.	Funcionalidad
EDT8.1	Poder actuar únicamente como una aplicación de sistemas de proveedor
EDT8.2	Poder ser desplegado como un sistema distribuido
EDT8.3	Poder ser desplegado como un procesador de tercera parte

Diccionario 74. EDT9 Especificación funcional del subproceso: Ambiente de arquitectura

De acuerdo a la especificación de la Arquitectura tecnológica

Diccionario 75. EDT10 Especificación funcional del subproceso: Soporte a procesos de negocio: Multiaplicaciones y almacenes de datos

Ref.	Funcionalidad
EDT10.1	Ejecutar aplicaciones y almacenes de datos de una o múltiples entidades
EDT10.2	Almacenar el código de las aplicaciones de una entidad con acceso a los datos de las aplicaciones de otra entidad. En este escenario, allí deberá ser definido un proceso, método de transporte seguro y acuerdos de nivel de servicio para proporcionar los datos para el SGTI, en un modo apropiado para realizar la reemisión, reemplazo de tarjeta y necesidades de descarga
EDT10.3	Definir los procesos, método para transporte seguro y acuerdo de nivel de servicios para proporcionar el código de las aplicaciones y datos para el núcleo del ambiente del SGTI de una manera consistente. Reemisión de tarjetas, reemplazo de tarjetas y necesidades de descarga de las aplicaciones, necesitan ser consideradas, de modo que esta configuración esté disponible para procesos de modo local
EDT10.4	Priorizar los recursos de las tarjetas para aplicaciones de tercera parte que son ubicadas en la tarjeta en etapa de postemisión del ciclo de vida de la tarjeta. Estas aplicaciones son descargables en un periodo posterior, las aplicaciones actuales y los datos típicamente residen en el sistema principal del proveedor de aplicaciones. Él titular típicamente también tiene igual trato con el proveedor de aplicaciones
EDT10.5	Reinstalar las aplicaciones sin datos de personalización. El ambiente del SGTI deberá de asegurarse del transporte seguro de la tarjeta a otra entidad para ubicar los datos de la aplicación en la tarjeta antes de que ésta sea embarcada al titular. Esto puede requerirse para aplicaciones o datos que requieren altos niveles de seguridad o privacidad
EDT10.6	Atender múltiples entidades empresariales que deberán almacenar aplicaciones y datos, de manera segura enviar estos a un procesador de tercera parte para procesamiento de emisión o reemisión
EDT10.7	Atender, para enviar un bloqueo de una aplicación, bloqueo de tarjetas o instrucciones de estado de tarjeta terminada a subsistemas de tercera parte
EDT10.8	Atender, para recibir bloqueo de aplicaciones, bloqueo de instrucciones de estado de tarjetas terminadas desde un subsistema de tercera parte

Diccionario 76. EDT11 Especificación funcional del subproceso: Ambientes distribuidos

Especificaciones de acuerdo a la Arquitectura tecnológica.

Diccionario 77. EIO1 Especificaciones funcionales del subproceso: Soporte a facturación

Ref.	Funcionalidad
EO25.1	Calcular los honorarios basados en el tamaño de cada aplicación, basados en el periodo en el cual la aplicación reside en la tarjeta, por requerimientos de seguridad o por descarga de aplicaciones
EO25.2	Mantener los enlaces al perfil de las aplicaciones en términos de cuando empieza y cuando termina, facturando las descargas y archivos borrados
EO25.3	Tener la capacidad para hacer los cargos de honorarios de los proveedores de aplicaciones y a los emisores
EO25.4	Ser interfaz con el sistema general de contabilidad y sistema de facturación de la organización
EO25.5	Producir reportes de facturación y opcionalmente de pedidos

De acuerdo a los requerimientos, criterios de costos de procesamiento de transacciones y niveles de servicio acordados.

Diccionario 78. EIO2 Especificación funcional del subproceso: Gestión de la calidad

Documentación de procesos y procedimientos conforme al estándar ISO 9001:2008.

Diccionario 79. EIO3 Especificación funcional del subproceso: Gestión de la seguridad de la información

Documentación de procesos y procedimientos conforme al estándar ISO/IEC 27001.

Los diccionarios de las especificaciones funcionales están resumidos en la tabla 33.

Tabla 33. Diccionarios de especificaciones funcionales

Diccionarios de especificaciones funcionales
EL1: Subproceso: Soporte a procesos de negocios: Administración del inventario de tarjetas
EO3: Subproceso: Definición y registro de la tarjeta
EO4: Subproceso: Definición y registro de aplicaciones

Diccionarios de especificaciones funcionales
EO5: Subproceso: Definición del Portafolio (Cartera)
EO6: Subproceso: Compatibilidad del portafolio
EO7: Subproceso: Preparación para la producción
EO8: Proceso de producción
EO9: Subproceso: Habilitación de la tarjeta
EO10: Subproceso: Preparación de datos/personalización
EO11: Subproceso: Postpersonalización
EO12: Subproceso: Terminación de la producción
EO13: Procesos de Postproducción
EO14: Subproceso: Gestión del ciclo de vida de la tarjeta
EO15: Subproceso: Gestión del ciclo de vida de las aplicaciones
EO16: Subproceso: Interfaz con otros sistemas
EO17: Subproceso: Postemisión: Descarga de aplicaciones
EO18: Subproceso: Postemisión: Canales de descarga de aplicaciones
EO19: Subproceso: Postemisión: Descarga segura de aplicaciones
EO20: Subproceso: Postemisión: Recuperación de errores en la descarga de aplicaciones.
EO21: Subproceso: Postemisión: Reemisión de tarjetas
EO22: Subproceso: Postemisión: Administración delegada
EO23: Subproceso: Postemisión: Procesos de usabilidad del titular de la tarjeta
EDT1: Subproceso: Soporte a procesos de negocio: Administración de llaves
EDT2: Subproceso: Soporte a procesos de negocio: Control de acceso
EDT3: Subproceso. Soporte a procesos de negocio: Archivo
EDT4: Subproceso: Soporte a procesos de negocio: Reportes
EDT5: Subproceso: Soporte a proceso de negocios: Arquitectura del sistema
EDT6: Subproceso: Soporte a proceso de negocios: Rendimiento
EDT7: Subproceso: Soporte a procesos de negocio: Interfaces externas
EDT8: Subproceso: Soporte a procesos de negocio: Consideraciones de implementación.
EDT9: Subproceso: Soporte a procesos de negocios: Ambiente de la Arquitectura
EDT10: Subproceso: Soporte a procesos de negocio: Multiaplicaciones y almacenes de datos
EDT11.Subproceso: Soporte a procesos de negocio: Ambientes distribuidos
EIO1 : Subproceso: Soporte a facturación
EIO2: Subproceso: Sistema gestión de la calidad
EIO3: Subproceso: Sistema gestión de la seguridad de la información

b) Línea base de la Arquitectura de aplicaciones

El estado actual que presenten las aplicaciones de los sistemas que atienden los requerimientos de negocio, su organización y estructura proporcionan los elementos para la conformación de la Línea base de aplicaciones.

Teniendo en cuenta la diversidad de entidades empresariales involucradas, el ambiente de los procesos centralizado o descentralizado y diferentes tecnologías, se deberá de realizar el inventario correspondiente, el cual deberá de contener lo siguiente:

- Entidad involucrada
- Dominios de la arquitectura de negocio en que participa
- Características de las aplicaciones:
    - Dominio de la arquitectura de negocios que atienden
    - Ambiente de operación: centralizado/descentralizado
    - Interfaces físicas de comunicación
    - Interfaces lógicas de comunicación
    - Administrador de base de datos
    - Aplicaciones propias, segunda o de tercera parte
    - Tipos de licenciamiento
    - Soporte y mantenimiento que se requiera
    - Requerimientos de plataforma
    - Personal especializado
    - Factibilidad de migración a tecnologías vigentes
- Diagramas de contexto y diagramas de flujo de datos
- Documentación de operación y técnica
- Planes de continuidad del negocio
- Estructura de las aplicaciones

c) Arquitectura de las aplicaciones

De acuerdo al dominio de las especificaciones funcionales, las podemos agrupar modularmente de la siguiente forma:

- Funcionalidades de administración de los diferentes componentes que integran el SGTI, tales como perfiles de tarjetas y aplicaciones, portafolios de productos y soluciones, usuarios del sistema, entidades empresariales involucradas, así como los privilegios que poseen o se les otorgan para su acceso al sistema

- Funcionalidades de ejecución de tareas especificas que modifican los estados del ciclo de vida de las tarjetas y las aplicaciones, así como las actividades que influyen sobre entidades que son autoridades en los procesos internos, tales como el Administrador de la tarjeta, los dominios de seguridad y aquellas actividades donde su ejecución es realizada por entidades empresariales como el proveedor de aplicaciones y el cargador/descargador de aplicaciones

- Funcionalidades que dan soporte a las actividades que modifican los estados de los ciclos de vida, desde la preparación del ambiente, las validaciones técnicas o de negocios, la ejecución de la transferencia de datos entre los estados y los componentes, el monitoreo de los procesos de carga/descarga hasta el reporte de éxito y de recuperación de las mismas al SGTI

- Funcionalidades que se requieren en el ambiente exterior a las tarjetas y que tienen impacto directo a la infraestructura y su comportamiento, así como fuente de información para el monitoreo de la administración de la infraestructura.
  El ambiente SGTI, tiene el alcance de incorporar aquellas actividades que no están automatizadas y que requieren soporte desde el mundo exterior a la tarjeta

A partir del análisis de brechas entre la Línea base de la arquitectura de aplicaciones y los requerimientos funcionales se determina la primera versión de la arquitectura de aplicaciones.

De acuerdo con Pressman [3], el estilo arquitectónico permite al diseñador de las aplicaciones (del software) obtener una estructura de programa que resulte relativamente fácil modificar y cambiar de tamaño, con este criterio, para los propósitos de esta tesis seleccionamos la arquitectura de programa principal/subprograma, la cual separa la función en una jerarquía de control donde un programa "principal" invoca a varios componentes.

Este programa principal, se representa por el menú de las opciones o funciones que el sistema otorga, por tanto, la arquitectura de las aplicaciones queda estructurada según la tabla 34.

Los diccionarios de los requerimientos funcionales se agrupan según al módulo de funcionalidad que le corresponda, para el caso de que todas las funcionalidades correspondan a un dominio la nomenclatura que se adopta es "número de diccionario.X", ejemplo EO16.X.

Tabla 34. Estructura de la arquitectura de las aplicaciones

Tipo de funcionalidad (menú principal)	**Requerimientos funcionales**	**Aplicados a:**
Administración	EO3.1,EO3.2,EO.7,EO4.1,EO4.2,EO4.5,EO5.1,EO5.2,,EO5.4,EO5.5,EO5.6,EO5.8,EO7.3,EO7.4,EO10.7,EO14.2,EO14.3,EO15.2,EO15.3,EO16.9,EO17.1,EL1.	Usuarios: Acceso, permisos y privilegios Entidades empresariales: roles Perfiles de: Plataformas, tarjetas, aplicaciones de

Tipo de funcionalidad (menú principal)	Requerimientos funcionales	Aplicados a:
Administración	X,EIO1.X, EDT4.X	tarjetas Mantenimiento al portafolio de productos Mantenimiento a catálogos Reportes Consultas
Reglas de las operaciones del ciclo de vida de la tarjeta y las aplicaciones	EO3.5,EO3.6,EO4.3,EO4.6,EO4.9,EO6.1,EO6.2,EO6.3,EO6.4,EO6.5,EO6.6,EO7.2,EO7.2,EO7.5,EO9.3,EO10.1,EO10.2,EO10.3,EO10.4,EO10.5,EO10.6,EO11.1,EO11.2,EO14.1,EO14.4,EO14.5,EO14.6,EO14.8,EO15.1,EO15.4,EO15.7,EO16.2,EO14.8,EO15.1,EO15.4,EO16.2,EO16.5,EO16.6,EO16.10,EO17.14,EO19.5,EO19.7	Gestión del ciclo de vida de tarjetas y aplicaciones Mantenimiento de aplicaciones Actualización de estados de los ciclos de vida de las tarjetas y aplicaciones Autorización de cambios de estado del ciclo de vida Administración a conflictos entre plataformas, aplicaciones, espacios de memoria
Soporte a las reglas de operación	EO3.4,EO4.4,EO5.3,EOA11.3,EO12.1,EO12.2,EO12.3,EO14.7,EO14.9,EO15.5,EO15.6,EO16.1,EO16.3,,EO16.7,EO17.8,EO17.10,EO17.11,EO17.12,EO19.1,A19.2,EO19.4,EO19.6,EO19.8,EO20.4,EO21.1,EDT1.X,EDT3.X,EDT7.X,EDT10.X	Preparación y ejecución de la carga/descarga de aplicaciones Gestión de parámetros Preparación del ambiente para la operación del ciclo de vida de tarjetas y aplicaciones Ejecución de operación sobre los estados del ciclo de vida Administración del estado de los resultados de las operaciones de carga/descarga/recuperación de errores en tarjetas y aplicaciones Cumplimiento de estándares para intercambio y transmisión de datos
Soporte al SGTI	EO9.1,EO9.2,EO16.4,EO16.8,EO17.2,EO17.3,EO17.4,EO17.5,EO17.6,EO17.7,EO17.9,EO17.13,EO17.14,EO18.1,EO18.2,EO18.3,EO18.4,EO18.5,EO19.3,EO19.8,EO19.9,EO19.10,EO20.1,E	Respaldo Recuperación Importación y exportación de archivos Configuración de interfaces Acceso a sistemas externos

Tipo de funcionalidad (menú principal)	Requerimientos funcionales	Aplicados a:
Soporte al SGTI	O20.2,EO20.3,EO20.5,EO22.X, EO23.X,EDT5.X,EDT6.X,EDT9. X, EDT11.X	Seguridad Interfaz con sistema administrador de llaves Administración de la infraestructura, configuración, capacidades, rendimiento preparar auditorías
Soporte a la operaciones manuales	EO4.7,EO4.8,EO4.10,EO4.11,E O5.9,EO5.10,EO5.11,EO5.12,E O5.13,EO7.6,EO7.7,EO9.5,EO9 .6,EO9.7,EO9.8,EO10.8,EO10.9 ,EO10.10,EO11.4,EO12.4,EO12 .5,EO17.16	Actividades de supervisión, control, verificación, validación

Arquitectura de datos

d) Estructura entidad-relación

En el apartado 3.3 y figura 30, se menciono la interacción entre las diferentes entidades empresariales que están involucradas en el ambiente del SGTI.

De acuerdo con Global Platform, la figura 54 muestra las principales relaciones entre las entidades empresariales.

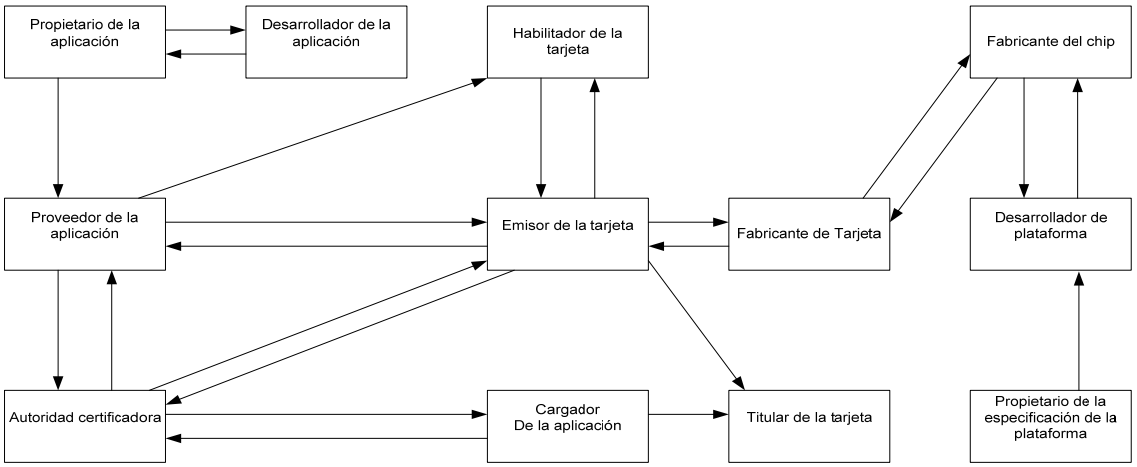


Figura 54. Relación entre lass entidades empresariales que participan en la operación del SGTI

El diccionario 80, resume las principales entidades y los roles con que participan en el SGTI.

Diccionario 80. DA Entidades empresariales involucradas en el SGTI

Entidades empresariales	Roles
Propietario de la aplicación (PA)	Es propietario de la aplicación y de la especificación, es responsable del desarrollo de los requerimientos y tipos de pruebas. Este rol lo desarrollan los dueños de los negocios (financieros, campus universitarios, gobierno o un innovador en negocios) Pudiera en algún caso tener derechos de autoría
Desarrollador de la aplicación (DA)	Escribe el código de la aplicación de acuerdo a los requerimientos y especificaciones proporcionadas por el propietario de la aplicación. Este rol lo desempeñan las áreas especializadas de desarrollo de software para tarjetas
Proveedor de la aplicación (PVA)	Provee los componentes necesarios para cargar una aplicación completa en la tarjeta. Tiene una relación directa de negocios con el propietario de la tarjeta y provee servicios para soportar la operación del propietario. Juega un rol similar a proveedores de servicios en donde él es el responsable de definir los servicios de las tarjetas. Las entidades empresariales que juegan este rol son emisores de tarjetas tradicionales, operadores de esquemas de lealtad, oficinas de gobierno, o autoridades de certificación que administran infraestructuras de llave publica
Cargador de aplicaciones (CA)	Carga a la tarjeta con aplicaciones y/o datos de personalización de acuerdo a las instrucciones del proveedor de aplicaciones, cumpliendo con las políticas de seguridad y un conjunto de procedimientos del emisor de la tarjeta. Es importante notar que este rol lo pueden jugar diferentes entidades desde la carga inicial de aplicaciones y

Entidades empresariales	Roles
Cargador de aplicaciones (CA)	carga post emisión de aplicaciones. Los actores inicialmente son proveedores de un buro de servicios, incluyendo carga de datos, personalización y servicios de personalización. Son proveedores de servicios de la industria de tarjetas y pueden ser vía modo local o de manera remota
Habilitador de la tarjeta (HT)	Prepara la plataforma y subsecuente carga de aplicaciones y es el responsable de la administración de las llaves. Los actores que juegan este rol son inicialmente operadores de buros de servicio, incluyendo carga de datos de manufactura y servicios de personalización. Actualmente los fabricantes de tarjetas juegan este rol
Emisor de la tarjeta (ET)	Es el responsable de manejar todos los procesos de producción de pre emisión incluyendo la selección del portafolio de aplicaciones para ponerlo a disposición de los propietarios. También es responsable de varios procesos de post emisión incluyendo el decomiso final de la tarjeta. Tiene una obligación legal asociada con los servicios a la tarjeta. Los actores que juegan este rol son Instituciones Financieras, Operadores de Transporte, Compañías de Telecomunicaciones Campus Universitarios ´´u Oficinas de Gobierno
Fabricante de la tarjeta (FT)	Es la entidad que fabrica la tarjeta de acuerdo a los requerimientos del emisor. Este rol es principalmente para la administración de materiales. Está coordinado con el cargador de la aplicación es y habilitador de la tarjeta. Los fabricantes de tarjetas generalmente son cuidadosos en el arte y ensamble de los procesos de embeber el chip. Los actores que juegan este rol son entidades

Entidades empresariales	Roles
Fabricante de la tarjeta (FT)	empresariales que actualmente están involucrados en la industria de las tarjetas
Titular de la tarjeta (TT)	Es el usuario final de la tarjeta y de los servicios proporcionados por el proveedor de aplicaciones, de acuerdo a los términos y condiciones del emisor de la tarjeta y proveedores relevantes de aplicaciones
Fabricante del chip (FC)	Fabrica las placas que contienen los chips con una configuración específica de ROM como fue diseñada por el desarrollador de la plataforma. El fabricante del CI controla los procesos de enmascarado y entrega los chips con las llaves iníciales de transporte y/o certificados para el fabricante de la tarjeta. Los actores que juegan este rol son inicialmente fabricantes de circuitos integrados para la industria de chips para tarjetas
Desarrollador de la plataforma (DP)	Escribe el código necesario para implementar los requerimientos de la especificación de la plataforma para un dispositivo particular de silicón proporcionado por el fabricante de CI. Los actores que juegan este rol son los que inicialmente desarrollan el código del ROM, para mascaras sobre circuitos integrados de la industria de tarjetas
Propietario de la especificación de la plataforma (PEP)	Desarrolla y mantiene los Derechos de propiedad Intelectual y provee detalles para un conjunto particular de especificaciones. Esto incluye las funciones de administración de la tarjeta, programación de aplicaciones de interfaces y funciones fuera de la tarjeta requeridas para facilitar la administración del ciclo de vida. Los actores que juegan este rol son organizaciones como Global Platform
Autoridad de la Administración de la	Es una parte que soporta al proveedor de aplicaciones para generar seguridad

Entidades empresariales	Roles
aplicación de llaves (AAA)	y liberar las llaves necesarias para operar la aplicación Los actores que juegan este rol pueden ser instituciones financieras, asociaciones de pago u organizaciones que proveen administración/certificación de llaves seguras
Autoridad de la Administración de la plataforma de Llaves (AAP)	Provee la plataforma para la administración relacionada con las llaves. Típicamente genera y mantiene la tarjeta, administra las llaves de tarjeta y llaves para el transporte Los actores que juegan este rol pueden ser emisores de tarjetas, instituciones financieras, asociaciones de pago, organizaciones que proveen servicios de certificación
Fabricante de la terminal (FT)	Fabrica las terminales con las diversas configuraciones de acuerdo a especificaciones de compatibilidad de las plataformas de tarjetas
Socios de negocio (SN)	Es aquella entidad que a partir de sus reglas de negocios sostiene una relación con el titular de la tarjeta y con los emisores de la misma. Opera parte de la infraestructura tecnológica
Operador del programa de tarjetas inteligentes (OPTI)	Administra las transacciones electrónicas vinculadas a las aplicaciones de los emisores
Colector de las transacciones electrónicas (CTE)	Integra y administra las transacciones electrónicas realizadas a través de la red de terminales, turnando en su caso posteriormente los resúmenes a cada operador o emisor de la tarjeta
Centro de autorización de transacciones electrónicas (CATE)	Válida y autoriza de acuerdo a reglas establecidas transacciones ejecutadas a través de aplicaciones de los diferentes socios de negocios o emisor de la tarjeta

La tabla 35 muestra las interseccionaes de las funcionalidades y roles de las entidades empresariales que participan en el SGTI

Tabla 35. Intersección entre funcionalidades y roles de las entidades empresariales del SGTI

	PA	DA	PVA	CA	HT	ET	FT	TT	FC	DP	PEP	AAA	AAP	FTR	SN	OPTI	CTE	CATE
PA	X	X	X															
DA	X	X																
PVA	X		X		X	X						X						
CA				X								X				X		
HT			X		X			X										
ET			X			X	X	X				X			X	X	X	X
FT						X	X		X					X				
TT						X		X							X	X		
FC							X		X	X								
DP									X	X	X							
PEP										X	X							
AAA			X	X		X						X	X					
AAP												X	X					
FTR							X							X				
SN						X		X							X	X	X	
OPTI			X		X		X								X	X	X	X
CTE						X									X	X	X	X
CATE						X										X	X	X

Las figuras 55 y 56 representan el mapeo de los correspondientes diagramas de contexto de los procesos para las tres etapas de producción, representadas en las figuras 42 y 43 respectivamente, desarrollados en la arquitectura de negocios.

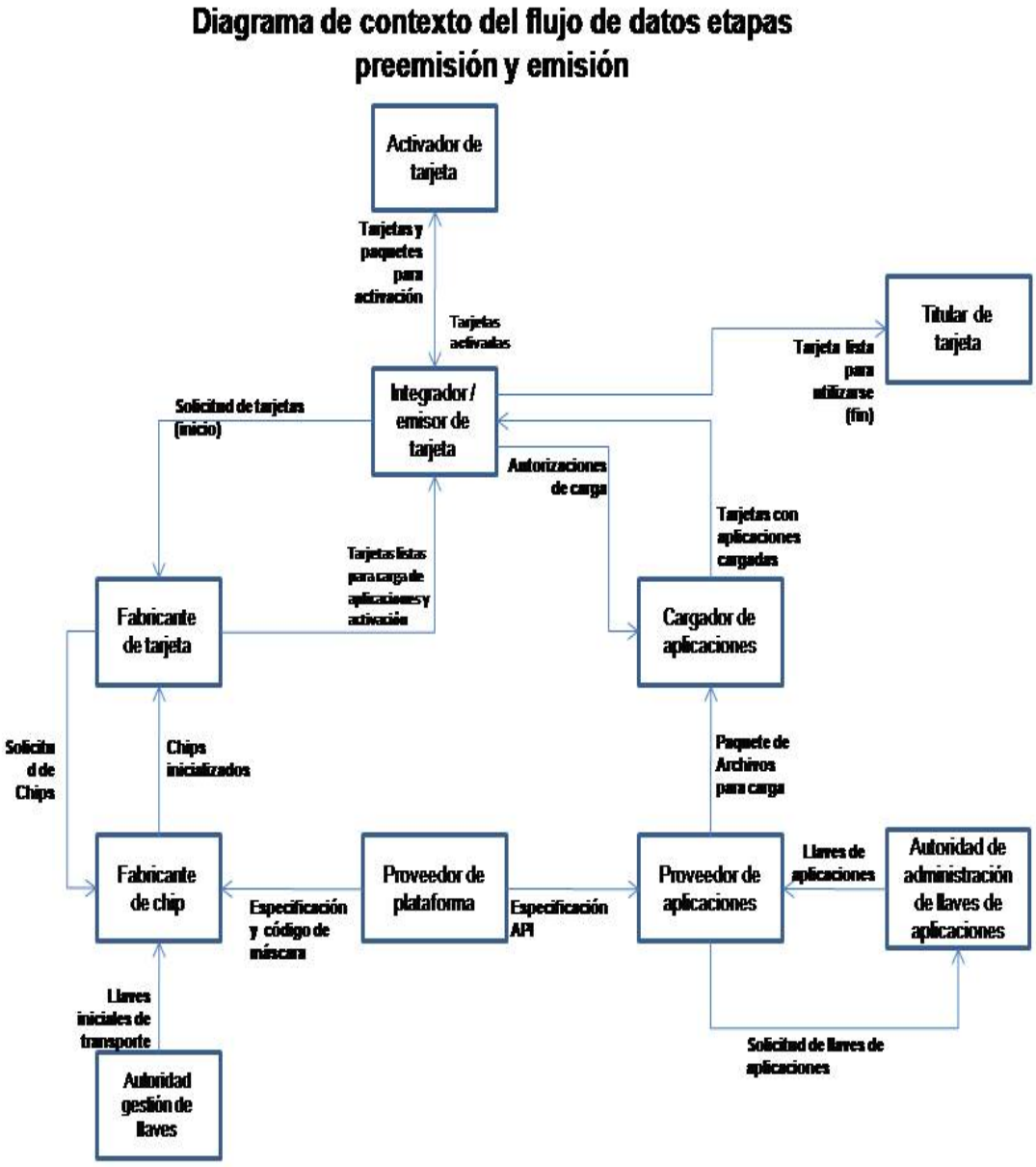


Figura 55. Diagrama de contexto del flujo de datos de los procesos de preemisión y emisión en el SGTI

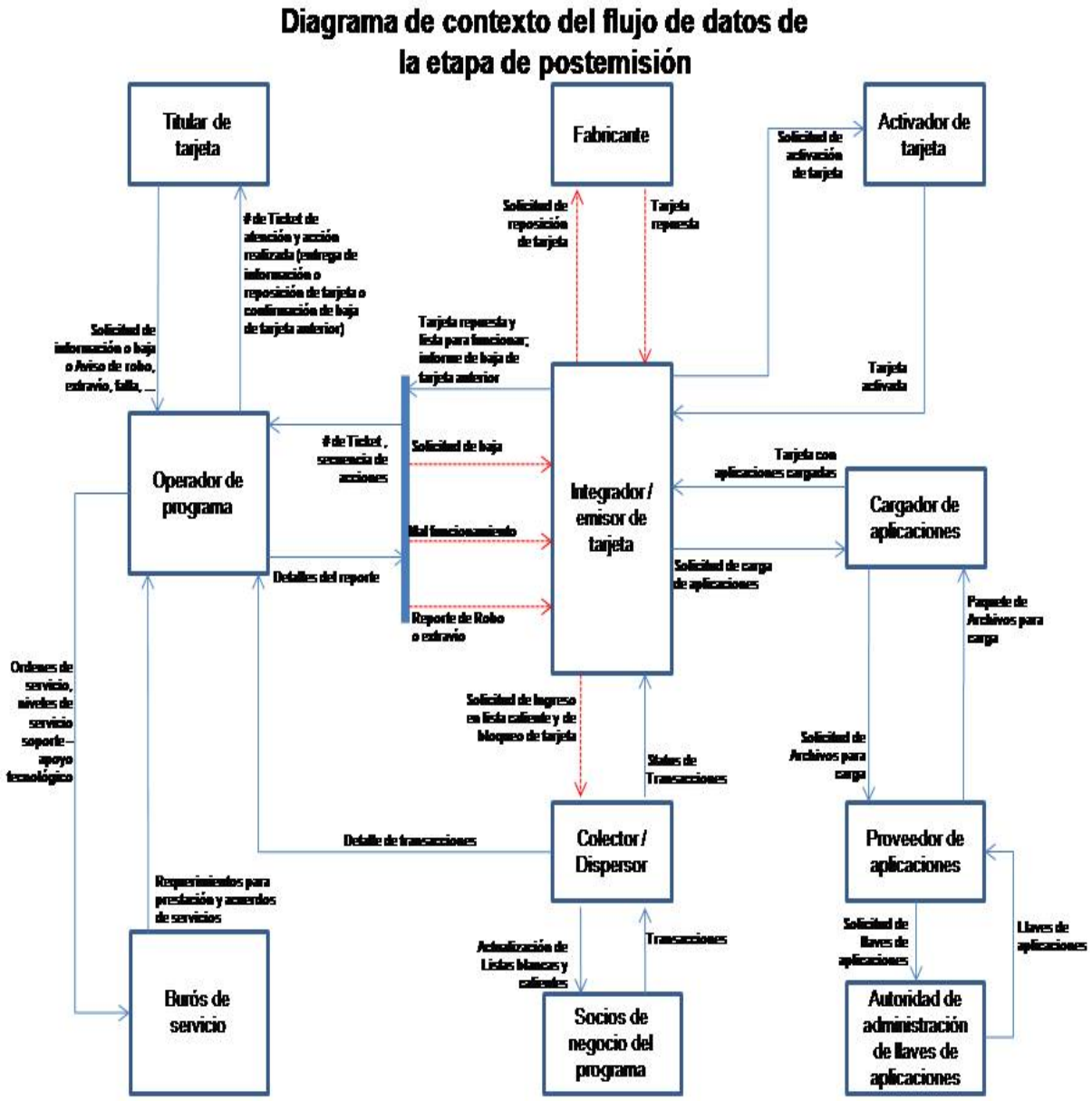


Figura 56. Diagrama de contexto del flujo de datos de los procesos de postemisión en el SGTI

e) Modelado de datos de las entidades empresariales involucradas: Estructura de datos

Diccionario 81. STD Estructuras de datos

Nombre entidad	Datos
Emisor de la tarjeta	Identificador de emisor
	Nombre del emisor

Nombre entidad	Datos
Titular de la tarjeta	Identificador de portafolio de productos
	Identificador de titular
	Nombre del titular
	Datos de georeferenciación
	Fecha de nacimiento
	Identificador de documento de identificación
	Fecha de documento de identificación
Habilitador de la tarjeta	Identificador del habilitador
	Perfil de habilitador
	Perfil de tarjetas que habilita
	Perfil de aplicaciones que habilita
Fabricante de la tarjeta	Identificador del fabricante de tarjeta
	Perfil de tarjetas que fabrica
	Nombre del fabricante
	Datos de georeferenciación
	Georeferencia de plantas donde fabrica tarjetas
	Portafolio de productos
	Contacto con clientes
Fabricante del CI	Identificador del fabricante del CI
	Nombre del fabricante de CI
	Portafolio de CI que fabrica
	Datos de georeferenciación
	Georeferencia de plantas donde fabrica CI
	Contacto con clientes
Desarrollador de la Plataforma	Identificador del desarrollador de Plataforma
	Nombre del desarrollador
Propietario de la especificación de la Plataforma	Identificador de Propietario
Proveedor de aplicaciones	Identificador de proveedor de aplicaciones
	Nombre del proveedor
	Datos de georeferenciación
	Perfil de aplicaciones
	Contacto con clientes
	Portafolio de aplicaciones
Propietario de las aplicaciones	Identificador de propietario de aplicaciones
	Nombre
	Datos de georeferenciación
Desarrollador de aplicaciones	Identificador de desarrollador
	Nombre del desarrollador
	Portafolio de aplicaciones
	Perfil de aplicaciones
Autoridad de la aplicación	Identificador de autoridad de gestión de llaves

Nombre entidad	Datos
de gestión de llaves	
Autoridad de la Plataforma de gestión de llaves	Identificador de plataforma de gestión de llaves
Cargador de aplicaciones	Identificador de cargador de aplicaciones
	Nombre del cargador de aplicaciones
	Datos de geo referenciación
	Portafolio de aplicaciones
	Perfil de aplicaciones
Proveedor de servicios	Identificador de proveedor de servicios
	Nombre de proveedor
	Datos georeferenciados
	Catálogo de servicios
Autoridad Certificadora	Identificador de la autoridad certificadora
	Nombre de la autoridad certificadora
	Datos de georeferenciación
	No de autorización
	Tipo de servicios que proporciona
Fabricante de terminales	Identificador de fabricante
Socios de negocios	Identificador de socio

Modelado de datos: Estructuras de datos: Componentes de tarjetas

Componente	Atributos
Tipo de tarjeta	Identificador del tipo de tarjeta
	Material de la tarjeta
	Tipo de microprocesador
	Sistema operativo de la tarjeta
	Tipo de acceso de la tarjeta
	Nivel de seguridad de la tarjeta
	Fabricante de la tarjeta
	Emisores de la tarjeta
Perfil de las tarjetas (Portafolio de tarjetas)	Identificador de perfil
	Tipo de tarjeta
	Aplicaciones primarias
	Estándares que incorpora
Tarjetas emitidas	CRN
	CIS
	Perfil de la tarjeta
	Identificador del titular de la tarjeta
	Titular de la tarjeta
	Datos de georeferencia del titular
	Pin

Componente	Atributos
Tarjetas emitidas	Estado del ciclo de vida de la tarjeta
	Aplicaciones primarias
	Aplicaciones secundarias
	Estados del ciclo de vida de las aplicaciones primarias
	Estados del ciclo de vida de las aplicaciones secundarias
	Fecha de expiración de la tarjeta
	Fechas de expiración de las aplicaciones
	Identificador de listas calientes
	Bitácora histórica de la tarjeta
	Máquina de producción
Tarjetas en producción	Identificador de orden de producción
	Número de pedidos relacionados
	Identificador del emisor
	Nombre del emisor
	Tipo de tarjeta
	Cantidad a producir
	Etapa de la producción
	Fecha estimada de fin de producción
	Identificador de las plantas de producción
	Bitácora de control de calidad
Pedido de tarjetas	Número de pedido
	Identificador del cliente
	Nombre del cliente
	Tipo de tarjeta
	Cantidad solicitada
	Fecha del pedido
	Fecha de entrega
Tarjetas en inventario	Identificador de la tarjeta
	Existencia
	Punto de reorden del inventario
	Cantidad mínima
	Cantidad máxima
	Fecha de último surtimiento
	Almacén
Orden de compra	
Microprocesador	Identificador del microprocesador
	Tipo de CI
	Velocidad del reloj
	Descripción del microprocesador
	Hardware
	Software
	Habilitación de seguridad

Componente	Atributos
	Fabricante
	Nivel de seguridad
Sistemas operativos	Identificador del S.O
	Proveedor del S.O
	Tipo de S.O.
	Descripción
	Especificaciones
	Versiones
	Requisitos de hardware
Perfil de las tarjetas (Portafolio de tarjetas)	Identificador de perfil
	Tipo de tarjeta
	Aplicaciones primarias
	Estándares que incorpora
Perfil de aplicaciones	Identificador del perfil de aplicaciones de tarjeta
	Tipo de aplicación
	Nombre de la aplicación
	Industria
	Tipo de tarjeta en que se carga
	Etapa de carga de la aplicación
	Cargadores de aplicación autorizados
	Perfil de infraestructura para carga
	Recuperación de carga
	Versión de la aplicación
	Soporte técnico
	Habilitación de seguridad
	Fecha de liberación
	Fecha de expiración
	Bitácora
	Medios de descarga

Modelado de datos: Definición de catálogos

Componente	Atributos
Catalogo de fabricantes de microprocesadores	Identificador de fabricante
	Datos generales del fabricante
	Contactos del fabricante
Catalogo de fabricantes de tarjetas	Identificador del fabricante
	Datos generales del fabricante
	Contactos del fabricante
Catalogo de equipamiento de plantas de CI	Identificador de planta
	Descipción de equipo 1
	Descripción de equipo 2
	Descripción de equipo n
Catalogo de	Identificador de planta

Componente	Atributos
equipamiento de plantas de tarjetas	Descipción de equipo 1
	Descripción de equipo 2
	Descripción de equipo n
Catalogo de máscaras (Sistema operativo)	Identificador de máscara
	Atributos de la mascara (i)
Diccionario de las reglas de negocio de los estados del ciclo de vida de las tarjetas	Definición del ciclo de vida
	Parámetros de gestión del ciclo
	Parámetros de gestión de los estados del ciclo
	Parámetros de los estados de transición del ciclo
	Condiciones de los estados
Diccionario de las reglas de negocio de los estados del ciclo de vida de las aplicaciones	Parámetros de gestión del ciclo
	Parámetros de gestión de los estados del ciclo
	Parámetros de los estados de transición del ciclo
	Condiciones de los estados
Diccionario de las reglas de negocio para listas calientes	Indicador de lista caliente
	Parámetros de la lista caliente
	Condiciones de los parámetros de lista caliente

Modelado de datos: Definición de registros de transacciones

Componente	Atributos
Registro para la personalización	Indicador de archivo
	Fecha de la personalización
	Número de registros
	Bitacora
Registro para la entrega de scripts para la personalización	Indicador de archivo
	Fecha de entrega
	Indicador de destino
	Indicador de éxito de entrega
Registro de las transacciones con operadores financieros	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de las transacciones con socios de negocio	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de transacciones con colectores de transacciones	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de transacciones con autoridad certificadora	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de transacciones con SGLL	Indicador tipo de transacción
	Fecha de entrega

Componente	Atributos
	Indicador de éxito de transacción
Registro de transacciones de carga de aplicaciones	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de transacciones de la respuesta a la carga de aplicaciones	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de transacciones a las peticiones del SGLL	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción
Registro de respuesta a las transacciones por parte del SGLL	Indicador tipo de transacción
	Fecha de entrega
	Indicador de éxito de transacción

f) Línea base de la Arquitectura de datos

Los sistemas de información en operación y sus diversas aplicaciones emplean la Arquitectura de datos que actualmente se encuentra definida. La estructura de los datos, los medios de almacenamiento, los contenidos de los datos, la calidad de los datos, entre otras son características que se habrán de documentar para tomar la decisión de migrarlos, realizar sobre ellos procesos de calidad de datos, implementar acciones de complemento de los mismos o en su caso más extremo volverlos a capturar

El análisis de brechas correspondiente dictará las acciones para integrar la Arquitectura de datos, a partir de lo existente y los requerimientos de negocio detectados para la nueva Arquitectura.

g) Arquitectura de datos

Tomando en cuenta los entregables de la fase, en este apartado se obtiene la Matriz jerárquica de funciones.

De acuerdo con Mylls [42] y Hares [43], la matriz jerárquica de funciones es parte de la arquitectura de datos (Tipo de entidad/Matriz funcional), la cual es un referente en las actividades del plan de migración, esta matriz se presenta a continuación:

Diccionario 82. DNE Nombre-Entidad

No.	Nombre entidad
E1	Emisor de la tarjeta
E2	Titular de la tarjeta
E3	Habilitador de la tarjeta
E4	Fabricante de la tarjeta

No.	Nombre entidad
E5	Fabricante del CI
E6	Desarrollador de la plataforma
E7	Propietario de la especificación de la Plataforma
E8	Proveedor de aplicaciones
E9	Propietario de las aplicaciones
E10	Desarrollador de aplicaciones
E11	Autoridad de la aplicación de la gestión de llaves
E12	Autoridad de la plataforma de gestión de llaves
E13	Cargador de aplicaciones
E14	Proveedor de servicios
E15	Autoridad certificadora
E16	Fabricante de terminales
E17	Socio de negocios
E18	Tarjeta emitida
E19	Pedido de tarjetas
E20	Orden de compra
E21	Perfil de las tarjetas (Portafolio de tarjetas)

Las entidades se categorizan de acuerdo a su funcionalidad de crear, leer, actualizar y borrar datos CLAB (CRUD por sus siglas en inglés, create, read, update, delete):

Matriz funcional jerárquica

Función de negocios	E 1	E 2	E 3	E 4	E 5	E 6	E 7	E 8	E 9	E 10	E 11	E 12	E 13	E 14	E 15	E16	E17	E18	E19	E20	E21
Logística de entrada														L		L			C	C	
Operaciones	C	L	A	C	C	C	L	C	L	A	A	L	C	A	A	L	A				C
Logística de salida	C	L	A	L	L	L	L	L	L	L	L	L	L	A	L	L	L	C			A
Mercadotecnia	L			L	L	L	L	L					L	A		A	L				A
Servicio	C	L	A	A	A	A	A	A	A	A	A	C	A	A	A	A	A				A
Adquisiciones																					
Recursos Humanos																					
Desarrollo Tecnológico	C	L	C	C	C	C	C	C	A	A	A	A	A	A	A	A	A	A			A
Infraestructura Organizacional	C	L	C	C	C	C	C	C	C	C	C	C	C	C	C	A	L				

La figura 57 muestra la estructura jerárquica de la Arquitectura de datos, formada por el diccionario de entidades, la estructura entidad/relación, los diccionarios de las estructuras de datos y la matriz jerárquica funcional.

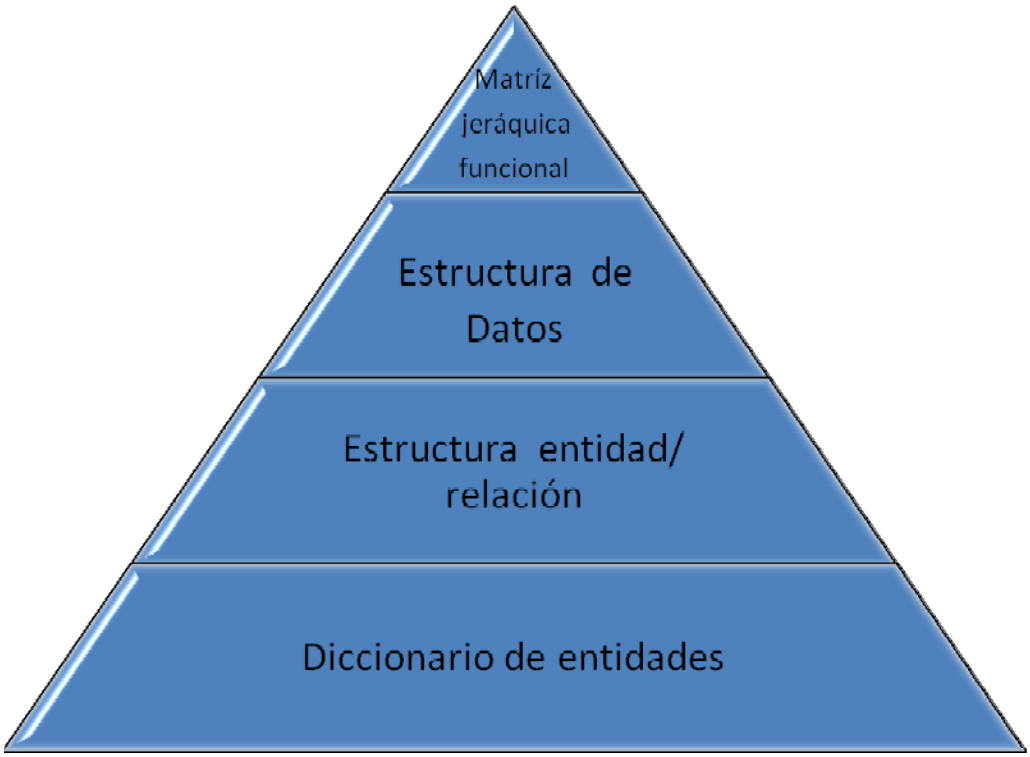


Figura 57. Estructura jerárquica de la arquitectura de datos

Fase D: Arquitectura tecnológica

De acuerdo con TOGAF, el objetivo de esta fase, es desarrollar una Arquitectura de tecnología que formará la base de la implementación de la nueva forma de trabajar

Los pasos para integrarla de acuerdo con TOGAF [W10] y Col Perks & Tony Beveridge [4] se ilustran en la figura 58, donde el modelo de referencia técnica (TRM por sus siglas en inglés, Technical Reference Model) sirve de guía para formular la Línea base de la arquitectura tecnológica.

El modelo de referencia técnica de TOGAF está representado en la figura 59, la cual presenta las capas de tecnología a considerar para el desarrollo y definición de la arquitectura tecnológica.

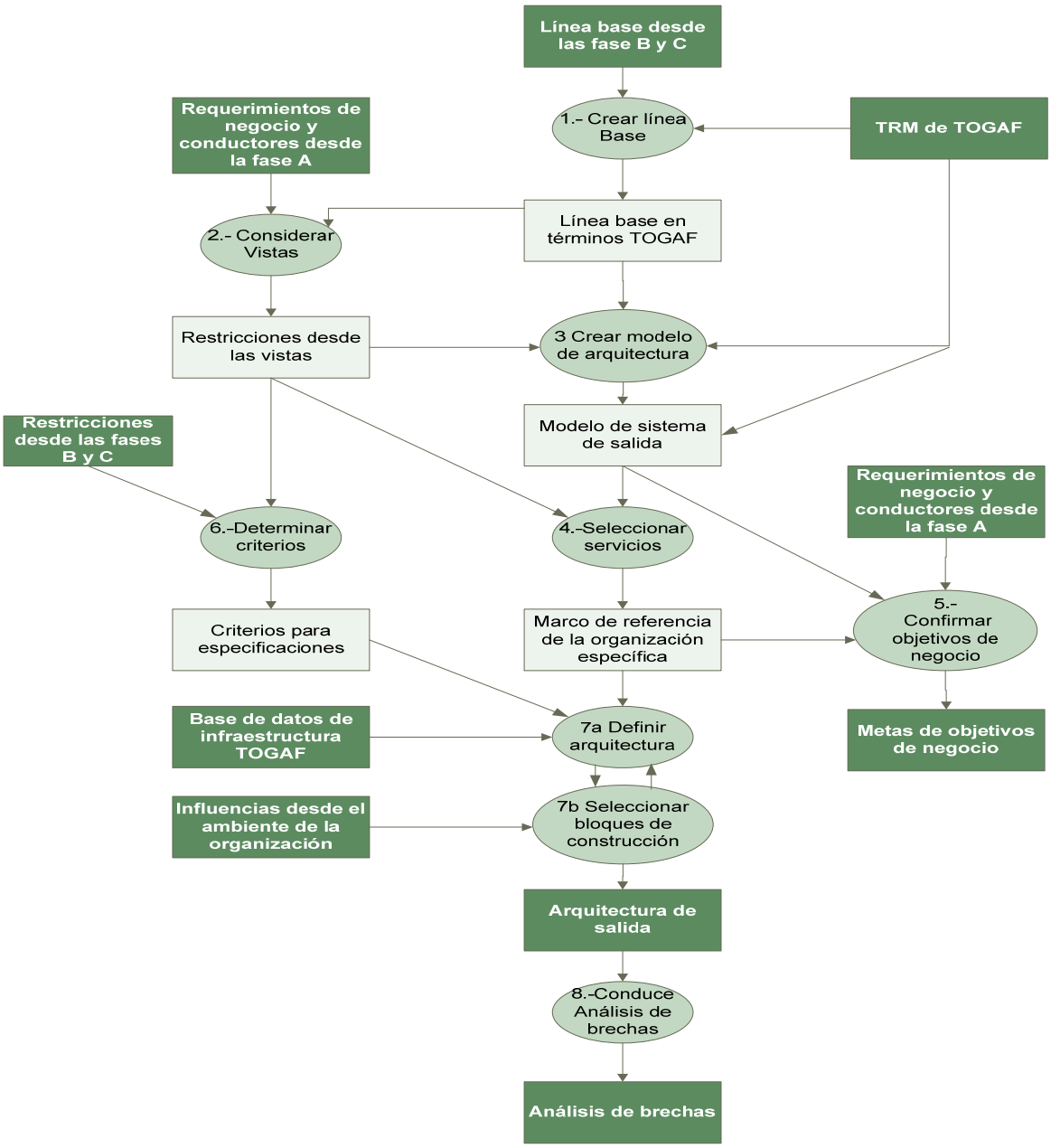


Figura 58. Flujo para la integración de la Línea base de la arquitectura tecnológica

a) Línea base de la Arquitectura tecnológica

El estado actual que presenta la infraestructura tecnológica de cada organización alineada al TRM, proporciona el inicio para la formulación de su Línea base.

Por tanto, cada una de las entidades involucradas en los procesos de la Arquitectura de negocios y del SGTI, deben de realizar el inventario de su infraestructura tecnológica, donde los componentes con una estructura de capas

sirven como punto de referencia para realizar el análisis de brechas entre las Arquitecturas actuales y propuesta.

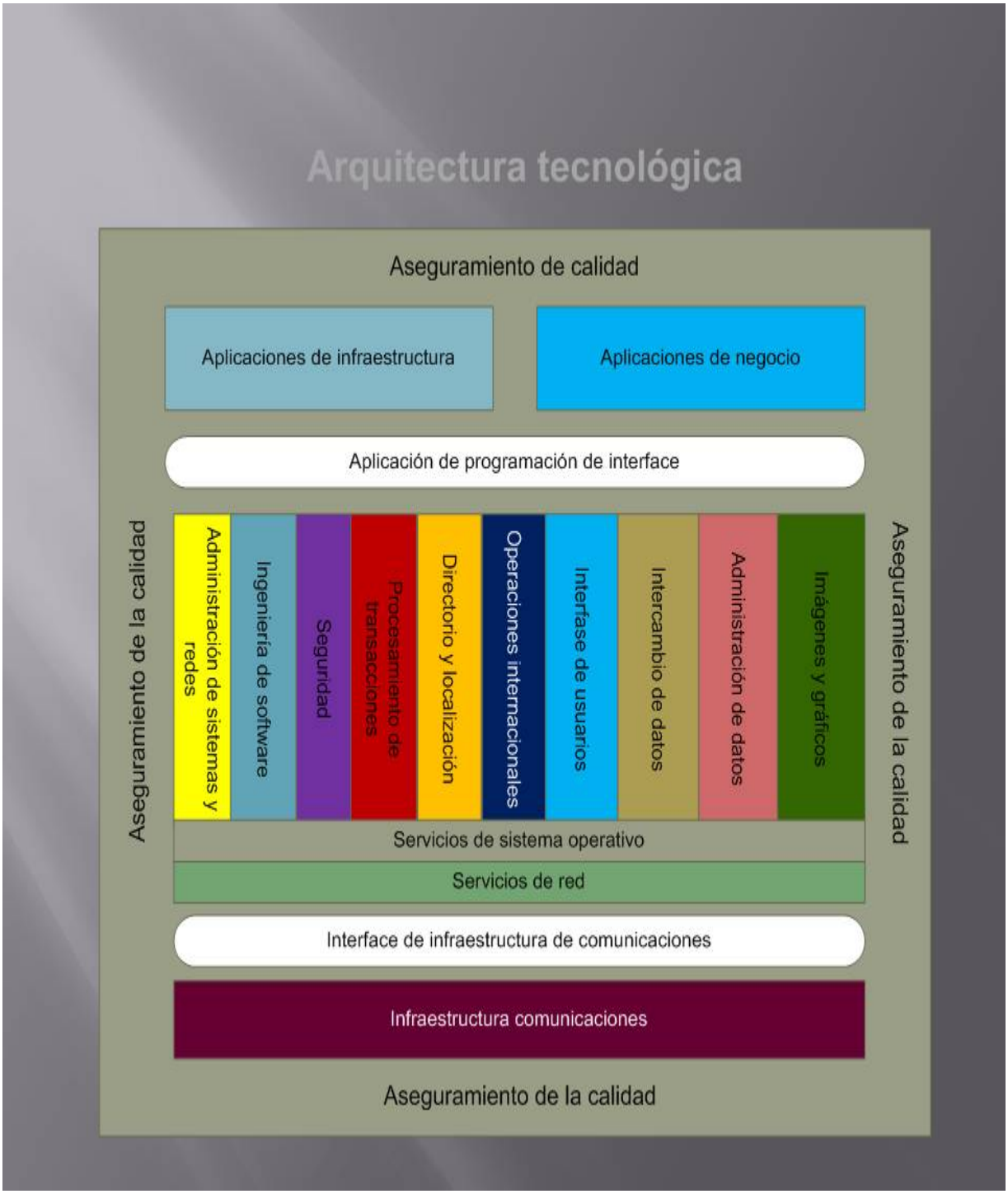


Figura 59. TRM de TOGAF, componentes y estructura de la arquitectura tecnológica

De acuerdo con la figura 58, se deben de tomar en cuenta como entrada para la definición de la arquitectura tecnológica propuesta, los requerimientos funcionales, los no funcionales y los de dominio, producto de las arquitecturas de negocio e información, descritas en los diccionarios correspondientes.

Los componentes referentes para realizar el análisis de brechas entre las Arquitecturas tecnológicas se describen en la tabla 36.

Tabla 36. Dominios de tecnología, según el TRM TOGAF

Capa de tecnología	Componentes
Calidad	Sistemas de gestión de la calidad, ISO 9001:2008, ISO/IEC 20000:2005 Administración de calidad de los datos
Infraestructura de comunicaciones	Redes, servidores de comunicaciones de datos
Interfaces de la infraestructura de comunicaciones	Switches, ruteadores, concentradores de puertos
Servicios de red	Internet, correo electrónico, mensajeria electrónica
Servicios de sistema operativo	Software base de sistema operativo de la plataforma Drivers y diversos componentes de software de aplicación compatible con el sistema operativo
Componentes tecnológicos	Administración de sistemas y redes Herramientas de software Hardware Seguridad Procesamiento de transacciones Ubicaciones y directorio Operación internacional Interfaz de usuario Intercambio de datos Administración de datos Gráficos e imágenes
Interfaz de aplicaciones de programación	Interfaces de la infraestructura de aplicaciones de las entidades empresariales involucradas
Aplicaciones de negocios	Sistemas de información de las entidades empresariales involucradas
Aplicaciones de infraestructura	Sistemas de administración de soporte, respaldo, recuperación

Un ejemplo de la matriz que integra el análisis de brechas, para la capa de calidad, se muestra en la tabla 37.

Tabla 37. Ejemplo del análisis de brechas, capa de calidad

Estado actual	Estado propuesto	Acciones a realizar
Los procesos actualmente están documentados al estilo de la organización, no hay consistencia y estandarización entre ellos	Los procesos y procedimientos deben de estar documentados como lo establece el control de documentos del estándar ISO 9001:2008	• Diseñar los procedimientos de control de documentos como lo establece el estándar seleccionado • Documentar de acuerdo al control de documentos establecido

b) b) Arquitectura Tecnológica
c)

Los requerimientos obtenidos a partir de la Arquitectura de negocios y los correspondientes a la Arquitectura de información son componentes de entrada al proceso de definición de la Arquitectura tecnológica (AT).

Como se refiere en la figura 58, las actividades señaladas como “restricciones desde las vistas”, “criterios para especificaciones” y “marco de referencia de la organización específica” así como el proceso “seleccionar servicios” requieren de procesos de gestión para su materialización física.

El estándar ISO/IEC 20000:2005 [W15] posibilita a los proveedores internos y externos de servicios de tecnologías de la información (TdeI) cómo mejorar la calidad de los mismos, para su entrega a sus clientes, tanto internos como externos.

A las diferentes entidades empresariales que están involucradas con la operación del SGTI, se les otorgan servicios de tecnología de la información, en este contexto se refiere a esta norma, como el estado del arte de la gestión de la infraestructura, la gestión, entrega y soporte de los servicios asociados a ella.

En la figura 58 se identifica una actividad como “criterios de especificaciones”, la cual es la definición a detalle de los requerimientos y funcionalidades de los servicios de sistemas y tecnología de la información para la configuración y capacidad de la AT.

Una de las principales funciones del SGTI, es el procesamiento de los estados del ciclo de vida de la tarjeta, la funcionalidad está expresada en términos de

reglas de negocio, entradas y salidas. Esto conlleva, tiempos de ejecución en diversos componentes, espacios de almacenamiento de datos, disponibilidad de los componentes de hardware y software, entre otros.

La figura 60 muestra la estructura y procesos de la norma ISO/IEC 20000:2005.

La norma ISO/IEC 20000:2005, Gestión de los servicios de tecnología de la información, está compuesta por dos partes, en la parte 1 se define la especificación para la gestión de los servicios de tecnología de la información, mientras que la parte 2 está integrada por el código de práctica de la gestión de los servicios. El documento de soporte para la gestión del servicio de TdeI es la Biblioteca de infraestructura de TdeI (ITIL) [W14], la cual es una serie de guías sobre la entrega de servicios de TdeI que emite la Oficina de Comercio del Gobierno del Reino Unido.

De acuerdo con la parte 1 de la norma, uno de los objetivos de ésta es:

- Promover la adopción de un enfoque de procesos integrados con el objeto de entregar servicios gestionados para cumplir con los requisitos de la empresa y de los clientes.

En el marco de la norma se establece que:

> "la gestión de los servicios de TdeI son para darle soporte a una o más áreas" y la calidad de TdeI es el "grado de alineación entre los servicios entregados y las necesidades de la empresa".

Así mismo se define como sistema de gestión a "Un sistema para establecer una política y objetivos, así como lograr estos".

La norma está estructurada por tres bloques:

- La planeación e implementación de la gestión de los servicios
- La planeación e implementación de servicios nuevos y,
- Los procesos para la gestión de servicios de TdeI

La norma tiene un enfoque a procesos de acuerdo al ciclo de Deming: planear, hacer, verificar y actuar. En el caso del primer bloque:

- Planear: Se lleva a cabo la planeación de la implementación y entrega de la gestión del servicio
- Hacer: Implementar los objetivos y el plan de gestión del servicio
- Verificar: Monitorear y medir que se logren los objetivos y el plan de gestión del servicio
- Actuar: Mejorar la eficacia y eficiencia de la entrega y gestión del servicio

El segundo bloque tiene como objetivo el asegurar que los nuevos servicios y las modificaciones se puedan suministrar y gestionar al costo y calidad del servicio acordados.

Para este bloque se deben considerar en las propuestas de servicios nuevos o modificados, el impacto organizacional, técnico, comercial y de costo. Los planes deben de incluir las funciones y responsabilidades para la implementación, operación, y mantenimiento de los servicios nuevos/modificados, la comunicación entre las partes relevantes, los requisitos de mano de obra y reclutamiento, así como las habilidades y capacitación, mediciones, métodos y herramientas del proceso, criterios de aceptación del servicio. Antes de la implementación el cliente del servicio debe aceptar los servicios nuevos/modificados, así también el proveedor debe informar sobre el resultado de los servicios, nuevos/modificados y compararlos con el plan, la revisión postimplementación debe realizarse a través de un proceso autorizado de cambios.

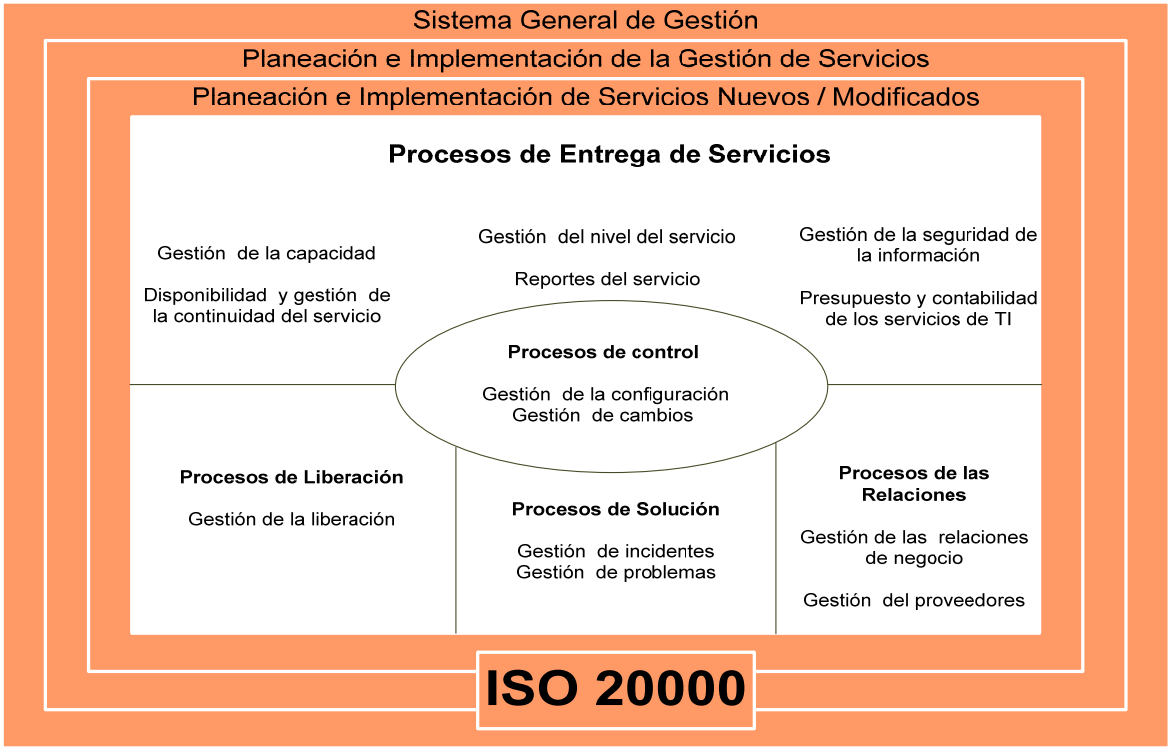


Figura 60. Estructura y procesos de la norma ISO/IEC 20000:2005

Los procesos y objetivos de esta norma se detallan en la tabla 38.

Tabla 38. Dominios, procesos y objetivos de la norma ISO/IEC 20000:2005

Dominios	Procesos	Objetivos
Entrega del servicio	Gestión de entrega del servicio	Definir, acordar, registrar y gestionar los niveles de servicio
	Reportes del servicio	Producir los reportes acordados, oportunos, confiables y exactos para la toma de decisiones informada y la comunicación eficaz
	Continuidad del servicio y gestión de la disponibilidad	Asegurar que la continuidad en los servicios acordados y los compromisos de disponibilidad se puedan cumplir bajo todas las circunstancias
	Presupuesto y contabilidad para los servicios	Presupuestar y registrar el costo de la entrega del servicio
	Gestión de la capacidad	Asegurar que el proveedor del servicio, cuente en todo momento con la capacidad suficiente para satisfacer la demanda acordada actual y futura de las necesidades comerciales del cliente
	Gestión de la seguridad de la información	Gestionar eficazmente la seguridad de la información en todas las actividades del servicio
Relaciones	Relaciones de negocios	Establecer y mantener una buena relación entre el proveedor del servicio y el cliente con base en la comprensión del cliente y los factores que impulsan su negocio
	Gestión de proveedores	Gestionar a los proveedores para asegurar la entrega de servicios transparentes de calidad
Solución	Gestión de incidentes	Restaurar a la empresa el servicio acordado lo antes posible o responder a las peticiones de servicio
	Gestión de problemas	Minimizar las interrupciones de la empresa al identificar y analizar proactivamente la causa de los incidentes y gestionar los problemas hasta su cierre
	Gestión de la configuración	Definir y controlar los componentes del servicio y la infraestructura y mantener información exacta de la configuración
	Gestión de cambios	Asegurar que todos los cambios se

Dominios	Procesos	Objetivos
Control		evalúen, aprueben implementen y revisen de forma controlada
Liberación	Gestión de la liberación	Suministrar, distribuir y rastrear uno o más cambios en una liberación en el medio ambiente vivo

Para la definición de la Arquitectura tecnológica los procesos de gestión que intervienen son el de gestión del nivel de servicio, disponibilidad y continuidad del servicio, capacidad, seguridad de la información y configuración.

Las recomendaciones para la implementación de la norma ISO/IEC 20000:2005, como lo plantea su parte 2 Código de prácticas, son emplear las mejores prácticas de la industria y del mercado, para el soporte y la entrega de los servicio de TdeI, en este sentido la mejor recomendación es utilizar la Biblioteca de infraestructura de TdeI (ITIL) [W14].

ITIL está formado por cinco libros, los cuales describen el ciclo de vida del servicio de TdeI:

- Estrategia del servicio: Proporciona recomendaciones sobre cómo utilizar la administración de servicios como herramienta estratégica para satisfacer las necesidades del negocio
- Diseño del servicio: Proporciona recomendaciones para el diseño de servicios (nuevos o modificados) y para el resto de los procesos de administración de servicios
- Transición del servicio: Proporciona recomendaciones para una transición fluida al introducir servicios nuevos y/o realizar modificaciones en los servicios dentro del entorno de producción
- Operación del servicio: Proporciona recomendaciones para alcanzar la entrega efectiva y eficaz, así como soporte de los servicios para garantizar el valor para el cliente y el proveedor de servicios, y,
- Mejora continua del servicio: Proporciona recomendaciones para mantener y mejorar el diseño, transición y operación del servicio, en línea con los cambiantes requerimientos del negocio

Los procesos que los integran son:

Libro	Procesos para la administración (de) (del)
Estrategia	• Portafolio de servicios • La demanda • Financiera
Diseño	• Catálogo de servicios • Nivel de servicios

Libro	Procesos para la administración (de) (del)
	• La disponibilidad • La continuidad del servicio • Proveedores • Seguridad de la información • La capacidad
Transición	• Cambios • Liberación y despliegue • La configuración y activos del servicio
Operación	• Incidentes • Problemas • Requerimientos • Accesos • Eventos
Mejora continua	Pasos para la mejora continua 1. Definir que se debería medir 2. Definir que se puede medir 3. Recopilar datos 4. Analizar datos 5. Presentar y usar información 6. Implementar acciones correctivas

Los procesos de estas prácticas que aplican en esta etapa de definición de la AT, son los siguientes:

- Estratégia del servicio y,
- Diseño del servicio

Por tanto la Arquitectura tecnológica estará integrada por los entregables de cada una de las actividades siguientes:

- Propuesta inicial de la AT a partir de las arquitecturas de negocio e información
- Incorporación de los resultados del análisis de brechas entre la Línea base y propuesta inicial de la AT
- Aplicación de los resultados que arrojen el marco de referencia de los procesos de dimensionamiento y gestión de servicios de TdeI
- Disposición de componentes en el mercado
- Resultado del análisis de servicios a contratar
- Trayectoria de capacitación y adiestramiento a los involucrados en la AT
- Diseño modular a nivel subsistemas para su despliegue y liberación

Fase E: Oportunidades y soluciones:

a) Versiones afinadas y actualizadas de la Visión de Arquitectura, Arquitectura de negocios, Arquitectura de información y Arquitectura tecnológica

En esta etapa de la construcción de la AEI, se debe de obtener el consenso de todos los involucrados, entidades empresariales internas y externas, de los modelos de Arquitecturas obtenidas.

El resultado del análisis de brechas entre los dos estados de la AEI proporcionará elementos, que deben de ser calificados para su incorporación, neutralización o eliminación, aunque esto tenga impacto en el alcance del proyecto.

Un proceso de retroalimentación debe de ocurrir para actualizar la AEI, lo que derivará en una nueva una versión que servirá al Plan de migración de la AEI.

b) Validación y consolidación de la Arquitectura

A partir de los acuerdos que se hayan obtenido para la incorporación de las modificaciones a la AEI se debe de obtener la validación por parte de las entidades empresariales involucradas y con autoridad delegada.

Esta validación provocara la versión final de la AEI.

c) Transición de la Arquitectura

En este punto de la trayectoria para iniciar la aplicación de la nueva AEI, se deben de identificar las actividades que aseguren la continuidad del negocio, así como la administración del riesgo que conlleva la adopción de una nueva forma de trabajo.

Se determinan aquellas actividades o procesos que deben de ocurrir en paralelo, para mitigar los riesgos que puedan ocurrir en una corrida individual de la nueva arquitectura.

d) Plan de migración

El plan de migración es un conjunto de actividades que se tienen que realizar en el tiempo, con responsables y participantes plenamente identificados, así como objetivos, hitos y metas por alcanzar.

En este contexto, como lo señala la Administración de proyectos según el Instituto de Administración de Proyectos (PMI por sus siglas en inglés) [W43], Gray [14], Chamoun [15] y Gido [16] en la etapa de gestión del tiempo, para el establecimiento del cronograma y ruta critica de la fase de planeación de la migración e implementación de la AEI, se deben de identificar los principales paquetes de trabajo a realizar (donde un paquete de trabajo es un conjunto

interdependiente de las actividades y resultados que ofrecen un resultado discreto de la empresa). Del análisis consensado de estos paquetes de trabajo se pueden obtener lagunas entre las actividades y las propuestas de solución, las cuales se deben de resolver en términos de las visiones de los todos los participantes.

Los paquetes de trabajo deben volver a agruparse en lo que respecta a las dependencias (incluyendo flujo de trabajo) y que este último análisis se utilice como base para la identificación de las actividades.

Siguiendo con Gray [14], Chamoun [15] y Gido [16], una vez que las actividades hayan quedado identificadas, la carta del proyecto y los estados del alcance de la migración deben de quedar claramente escritos.
Los beneficios también pueden ser ahora enmarcados en el contexto de toda la empresa, utilizando la arquitectura de la empresa. Alto retorno de inversión debe de ser identificado para mostrar el potencial de éxito temprano.
Durante este último paso, las especificaciones de los elementos básicos deben de verificarse que se cumplirán, es decir verificar que no haya ocurrido un desalineamiento con respecto a los requerimientos del negocio.

En este punto se tienen los paquetes de trabajo a considerar en el Plan de migración.

Fase F: Plan de migración

El objetivo de esta fase es ordenar por prioridad los componentes de la migración del SGTI. Las actividades incluyen la evaluación de las dependencias, los costos y beneficios de las actividades de migración, un ejemplo de lo anterior, que como resultado de la compatibilidad de intercambio de datos entre diversos equipos, habrá que diseñar/adquirir interfaces, desarrollar aplicaciones o migrar bases de datos a otros ambientes.

La mayoría de las organizaciones deben descubrir que un cambio de la Arquitectura tiene un importante impacto en la organización si se realizará en una única fase. La migración a menudo requiere la consideración de una serie de aspectos técnicos y no técnicos, los cuales están asociados con los medios de introducir cambios en los sistemas de operación.

Aspectos que requieren especial consideración pueden incluir:

- Las operaciones paralelas
- Las opciones de proceder a la migración gradual por subsistema o por función
- El impacto de la separación geográfica
- El destino futuro de los sistemas actuales
- Los requerimientos deben de ser combinados o divididos en partes para facilitar la secuenciación y la aplicación. Este reordenamiento de

aplicaciones crea una serie de proyectos, un proyecto equivalente a un requerimiento o combinaciones o partes de aplicaciones

Las decisiones resultantes de estas consideraciones deben ser incorporadas en el plan de ejecución. La estrategia básica es centrarse en paquetes/actividades que ofrecen entrega de resultados a corto plazo y crear así un impulso para un enfoque común consistente en implementar las funciones de negocios en una base de datos generada en orden cronológico, es decir, crear las aplicaciones y apoyo de la tecnología que creen los datos antes que las del procesamiento de datos, es decir antes que las que sean almacenar, archivar o borrar datos, es decir la Matriz de jerarquía de la arquitectura de datos.

La tabla 39 muestra los principales paquetes de trabajo del Plan de migración e implementación a realizar:

Tabla 39. Paquetes de trabajo del plan de migración:

a) Preparación de ambientes de operación	**Entidades empresariales involucradas**
Integración de los perfiles de tarjetas	Habilitador de la tarjeta Emisor de la tarjeta Fabricante de la tarjeta
Integración de los perfiles de aplicaciones	Propietario de las aplicaciones Desarrollador de las aplicaciones Proveedor de la aplicación Emisor de la tarjeta
Integración del portafolio de productos	Emisor de la tarjeta
Definición de los estados de transición del ciclo de vida de las aplicaciones	Emisor de la tarjeta Propietario de la aplicación Desarrollador de las aplicaciones
Definición de las reglas de negocios de los estados del ciclo de vida de las aplicaciones	Emisor de la tarjeta Propietario de la aplicación Desarrollador de las aplicaciones
Integración de los catálogos	Emisor de la tarjeta Fabricante de la tarjeta Fabricante del chip Fabricante de la terminal Socios de negocio
Definición de la configuración del sistema de gestión de llaves	Autoridad de la administración de la aplicación de llaves Autoridad de la administración de llaves
Definición de la configuración del HSM	Autoridad de la administración de la aplicación de llaves Autoridad de la administración de llaves
Definición de reglas de listas calientes	Emisor de la tarjeta Socios de negocios

a) Preparación de ambientes de operación	Entidades empresariales involucradas
Definición de los procesos para la recuperación de errores o fallas en descargas de aplicaciones en postemisión	Cargador de aplicaciones Habilitador de la tarjeta Emisor de la tarjeta
Definición de reglas para la compatibilidad de plataformas con portafolio de productos	Fabricante de la tarjeta Fabricante del chip Desarrollador de la plataforma Propietario de la especificación de la plataforma
Preparación de las interfaces lógicas con sistemas externos	Proveedor de la aplicación Socios de negocio
Preparación de interfaces físicas entre subsistemas internos	Emisor de la tarjeta
Preparación de interfaces lógicas entre sub sistemas internos	Emisor de la tarjeta
Definición de procesos para la administración delegada	Emisor de la tarjeta
Definición de la configuración de la infraestructura	Emisor de la tarjeta Proveedor de la aplicación
Definición de los privilegios de acceso al SGTI	Emisor de la tarjeta
Parametrización de componentes de software de aplicación	Desarrollador de la aplicación Proveedor de la aplicación
Parametrización de componentes de software base	Emisor de la tarjeta
Diseño de la red de comunicaciones	Emisor de la tarjeta
Definición de la parametrización de red de comunicaciones	Emisor de la tarjeta Socios de negocio
Definición de políticas para la seguridad de la información	Emisor de la tarjeta
Diseño de los componentes para la seguridad de la información	Emisor de la tarjeta Autoridad de la administración de llaves

b) Preparación del ambiente de la infraestructura	Entidades empresariales involucradas
Configuración de componentes de infraestructura	Emisor de la tarjeta Proveedor de la aplicación
Preparación de las interfaces físicas con sistemas externos	Emisor de la tarjeta Proveedor de la aplicación
Preparación de interfaces físicas entre subsistemas internos	Emisor de la tarjeta
Configuración de componentes de infraestructura de seguridad de la	Emisor de la tarjeta Autoridad de la administración de llaves

b) Preparación del ambiente de la infraestructura	Entidades empresariales involucradas
información	
Creación de esquemas de bases de datos	Emisor de la tarjeta Proveedor de la aplicación
Configuración de administradores de bases de datos	Emisor de la tarjeta Proveedor de la aplicación
Afinación de los componentes de hardware y software	Emisor de la tarjeta Proveedor de la aplicación
Configuración de infraestructura del SGLL	Autoridad de la administración de la plataforma de llaves
Configuración de infraestructura del HSM	Autoridad de la administración de la plataforma de llaves
Configuración de infraestructura de comunicaciones	Emisor de la tarjeta
Configuración de la infraestructura para la seguridad de la información	Emisor de la tarjeta

c) Prepación de aplicaciones para:	Entidades empresariales involucradas
Crear datos en las bases de datos	Emisor de la tarjeta Desarrollador de las aplicaciones
Leer datos de las bases de datos	Desarrollador de aplicaciones
Actualizar datos en las bases de datos	Desarrollador de aplicaciones
Borrar datos en las bases de datos	Desarrollador de aplicaciones

d) Realización de pruebas	Entidades empresariales involucradas
Definición y alcance de las pruebas	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Definición de participantes en las pruebas	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Preparación para la realización de las pruebas	Emisor de la tarjeta
Realización de las pruebas	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta

d) Realización de pruebas	Entidades empresariales involucradas
	Socios de negocios
Registro de los resultados de las pruebas	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Retroalimentación a las fases que correspondan	Emisor de la tarjeta

e) Preparación y migración de datos	Entidades empresariales involucradas
Determinación de datos a migrar	Emisor de la tarjeta Desarrollador de la aplicación
Identificación de componentes e interfaces a utilizar	Emisor de la tarjeta Desarrollador de la aplicación
Realizar migración de datos	Emisor de la tarjeta
Pruebas sobre datos migrados	Emisor de la tarjeta
Registro de resultados	Emisor de la tarjeta
Retroalimentación a las fases que correspondan	Emisor de la tarjeta

f) Capacitación y el entrenamiento	Entidades empresariales involucradas
Identificación y determinación de temas	Emisor de la tarjeta Socios de negocio
Identificación y determinación de los recursos humanos a capacitar	Emisor de la tarjeta Socios de negocio
Calendarizar la capacitación y el entrenamiento	Emisor de la tarjeta Socios de negocio
Realizar la capacitación	Emisor de la tarjeta

g) Transición de los servicios de TdeI	Entidades empresariales involucradas
Definir las unidades de liberación	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Elaborar trayectoria de servicios de TI en transición	Emisor de la tarjeta
Ejecutar la liberación de los servicios	Emisor de la tarjeta

h) Definición de la prueba piloto	Entidades empresariales involucradas
Definir alcance de la prueba piloto	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Identificar recursos necesarios para prueba piloto	Emisor de la tarjeta
Verificar recursos de prueba piloto	Emisor de la tarjeta
Realizar prueba piloto	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Registrar resultados de prueba piloto	Emisor de la tarjeta Proveedor de aplicaciones Desarrollador de aplicaciones Habilitador de la tarjeta Socios de negocios
Retroalimentar a las fases que correspondan	

i) Liberación a producción	Entidades empresariales involucradas
Programación de puesta en producción	Emisor de la tarjeta
Seguimiento y control de la producción	Emisor de la tarjeta
Administración de cambios	Emisor de la tarjeta
Administración de la mejora continua	Emisor de la tarjeta

Los paquetes de trabajo del Plan de migración están formados por un número importante de servicios de TdeI, es una característica intrínseca al propio paquete de trabajo en cuestión, en este ámbito, las actividades se realizan mediante la mejor práctica señalada por ITIL, en este caso la que aplica es la del diseño del servicio.

En el Anexo 3 se incluye el cronograma, hitos y ruta crítica del plan de migración.

Fase G: Gobierno de la implementación

Ejecutar la implementación del SGTI, requiere de los mecanismos que hagan efectivo su gobierno, el cual en esta propuesta metodológica estan integrados por:

a) Norma interna para ejercer el gobierno

A través de esta iniciativa se formaliza el marco regulatorio, para dar el seguimiento, control y evaluación del Plan de migración.

En ella se deben de establecer:

- El alcance del gobierno de la implementación
- El Comité de gobierno formado por representantes de las entidades empresariales involucradas en el SGTI
- Las reglas operativas del Comité
- Los mecanismos para el seguimiento, control y evaluación del plan
- Los mecanismos de comunicación formal entre los integrantes del Cómite y las diferentes partes interesadas

b) Recomendaciones para la ejecución del Plan de migración

En esta etapa es donde se reúne toda la información para el éxito de la gestión del proyecto. Teniendo en cuenta que en paralelo, se lleva a cabo la evolución de la organización, que es donde los cambios reales suceden.

En esta fase se establece la conexión entre la Arquitectura y la organización.

Aplican para la obtención de los entregables de esta fase, el proceso de gestión de la liberación como lo señala ISO 2000:2005 [W15] y la administración de la transición de servicios como lo establece ITIL [W14].

En el nivel más bajo de la estructura de la AEI, ocurren los servicios de TdeI. En tal sentido los servicios de TdeI juegan un papel importante en la migración.

Durante esta ejecución ocurren los cambios e impactos por la adopción de la nueva Arquitectura, la administración de la transición de los servicios incluye la administración de:

- Los cambios de los servicios
- La liberación y despliegue de los servicios
- La configuración de los activos de los servicios

Como lo señala ITIL [W14] y lo expone Piattini [40], la etapa de transición de los servicios de TdeI, debe de proporcionar recomendaciones para el desarrollo y la mejora de las capacidades necesarias para realizar una transición a los servicios

nuevos o modificados en el entorno de producción con la mayor transparencia posible para los usuarios.

Las metas y objetivos de estas actividades son:

- Planificar y gestionar los recursos para implantar con éxito un servicio nuevo o modificado en el entorno de producción con los costos previstos y dentro de las estimaciones de calidad y tiempo
- Garantizar que se produzca el menor impacto posible sobre los servicios en producción, las operaciones y la organización
- Aumentar la satisfacción del cliente con las prácticas de la transición de los servicios
- Aumentar el uso adecuado de los servicios, las aplicaciones subyacentes y las soluciones tecnológicas
- Proporcionar guías claras e integrales que permitan a los clientes, usuarios, entidades empresariales involucradas y al negocio cambiar sus actividades para alinearlas siguiendo los planes de transición

Los beneficios para los involucrados se tienen que reflejar en:

- Darle a la organización la capacidad de absorber una gran cantidad de cambios y versiones de una forma segura
- Gestionar la transferencia de servicios a, o desde un proveedor de servicio externo
- Alinear los servicios nuevos o cambiados con los requerimientos del negocio y de los clientes
- Garantizar que los clientes y usuarios pueden usar los servicios nuevos o modificados de forma que se maximice el valor de las operaciones del negocio

Las metas de la administración de los cambios son:

- Responder a los dinámicos requerimientos comerciales de los clientes, a la vez que se maximiza el valor y se reducen los incidentes, interrupciones y la duplicación de esfuerzos.
- Responder a las solicitudes de cambios del negocio y de las TdeI de forma que se alineen los servicios con las necesidades comerciales.

La premisa dentro de la administración de cambios, es que estos se registren, tengan el adecuado seguimiento y que de forma controlada sean:

- Evaluados,
- Autorizados,
- Priorizados,

- Planificados,
- Probados,
- Implementados,
- Documentados y,
- Revisados

Estos cambios forman parte del análisis de impacto. Los retos y beneficios de la administración de los cambios, los podemos agrupar como sigue:

Retos	Beneficios
Los detalles de configuración imprecisos llevan a una incorrecta evaluación de los cambios	Mejor alineación de los servicios con los requerimientos de los clientes
Su implementación es un proceso muy burocrático	Disminución del impacto negativo en la prestación de servicios como consecuencia de los cambios
Conectar los procesos de administración de cambios con el de administración de proveedores (internos y externos)	Plena comprensión del costo de los cambios
Intentos de pasar por alto el proceso	Capacidad para absorber un elevado nivel de cambios dentro de la organización
Procedimientos de marcha atrás incorrectos, inexistentes o sin probar	Mejora en la evaluación del riesgo de los cambios
El alcance del cambio es demasiado amplio	Mayor visibilidad y comunicación de los cambios
Se priorizan demasiados cambios como urgentes	Crear la cultura de que un cambio no aceptado es inaceptable

La Administración de la configuración de los activos del servicio, toma en cuenta a cada elemento de las Arquitecturas, los cuales son un activo, y todos deben de estar bajo el control de la Administración de la configuración.

En la Administración de la configuración se deben de tomar en cuenta otros conceptos tales como:

- La experiencia del personal
- El rendimiento de la organización
- El número y comportamiento de los usuarios
- La capacidad y expectativas de los proveedores y socios
- Los niveles y habilidades de los usuarios

La Línea base de la configuración debe de revisarse y acordarse formalmente y sólo podrá cambiarse mediante procedimientos de cambio formales

Los objetivos de la Administración de liberación y despliegue deben de garantizar que:

- Existan los Planes de liberación y despliegue necesarios para estar alineados con los clientes y el negocio en los proyectos de cambios
- Puedan crearse, instalarse, comprobarse e implementarse paquetes de versiones exitosamente dentro del plazo establecido
- Los servicios nuevos o modificados sean capaces de alcanzar los niveles de servicio acordados
- Se produzca la transferencia de conocimientos a los clientes, a los usuarios, al personal de operaciones y soporte
- Se produzca el menor impacto posible en los servicios del entorno de producción
- Los clientes, usuarios y personal de la administración de servicios estén satisfechos con las prácticas y salidas de la transición de los servicios.

Para las actividades de liberación se deberá de establecer la unidad de liberación, la cual describe la parte del servicio o infraestructura tecnológica que será liberada conjuntamente.

Las unidades de liberación deben de ser identificadas de una forma única.

La liberación debe de tener un diseño, puede ser:

- Bing-Bang, se implementa todo, servicios, aplicaciones, infraestructura a la vez
- Por fases, se implementa a diversos grupos de usuarios, aplicaciones e infraestructura en momentos diferentes
- Implementada desde una ubicación centralizada y se aplica a los usuarios, o se pone a disposición y son los usuarios los que deciden cómo y cuándo aplicarla según sus necesidades o se negocia una combinación de las anteriores

Según el modelo “V” (iniciando en el nivel 1 de los requerimientos y terminando en el nivel 1 de la liberación), la correspondencia entre las trayectorias de los requerimientos y la liberación son:

Nivel	Trayectoria del requerimiento	Trayectoria de la liberación
1	Necesidades de usuarios y clientes	Servicio de prueba y evaluación: El servicio soportará las necesidades

Nivel	Trayectoria del requerimiento	Trayectoria de la liberación
	del negocio	del cliente y el negocio
2	Requerimientos del servicio	Servicio de prueba: Puede el servicio cumplir con los criterios de aceptación
3	Solución del diseño del servicio	Preparación de la operación de servicios: Verifica que el objetivo de despliegue de la organización y gente esté dispuesta a desplegar y operar los nuevos o modificados servicios
4	Liberación del diseño del servicio	Probar liberación del servicio: Los componentes del servicio pueden estar integrados correctamente y la liberación puede estar construida y probada en el ambiente objetivo
5	Desarrollo de solución del servicio	Prueba de componentes: Componentes se ponen a prueba en forma aislada para garantizar que la entrega sea como se especifica

c) Documentación del avance de la Administración del Plan de migración

Mediante procedimientos automatizados o manuales realizar el seguimiento del Plan de migración, actualizando los avances, los entregables, las contingencias, los problemas no resueltos y las medidas acordadas para garantizar la continuidad del Plan.

d) Minutas de trabajo de revisión de avances

Expedir con oportunidad, para su revisión, validación y aprobación las minutas de trabajo y documentación derivada de las reuniones de avances de trabajo.

e) Recomendaciones y acuerdos de medidas para solventar desviaciones de la ejecución del Plan de migración

Registrar, validar y verificar, los acuerdos tomados durante sesiones de trabajo o sobre la marcha del conjunto de acciones que permitan redireccionar medidas de

contención, preventivas y/o correctivas, en su caso a través del mecanismo de administración de cambios.

f) Realizar el análisis de impacto

Para aquellas acciones que impliquen modificaciones que estén fuera de los parámetros autorizados del manejo presupuestal, tiempos u otros compromisos del avanmce, realizar el análisis de impacto, para darlo a conocer a las instancias correspondientes.

g) Seguimiento a medidas acordadas en reuniones de revisión previas

Validar y verificar los reportes de las reuniones previas e integrarlas en el expediente del plan de migración.

h) Acta de cierre de la migración

Como lo establece la Administración de proyectos, realizar el protocolo del cierre de la migración.

4.2.5 Actividades de retroalimentación del desarrollo de los entregables

a) Documentación de los resultados obtenidos de cada fase.

b) Anexar las lecciones aprendidas de cada fase.

4.3 Propuesta de Gobierno del SGTI

Para los propósitos de esta tesis, este apartado corresponde dentro del modelo de AEI de TOGAF a la Administración del cambio de arquitectura.

De acuerdo con el Instituto de Gobierno de Tecnología de la Información (IGTI) [W11], se entiende por Gobierno de TdeI,

> "al conjunto de acciones, que realiza el área de TdeI en coordinación con la Alta Dirección, para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio".

Otra definición de Gobierno de TdeI, la proporciona Piattini [40],

> "la gestión de TdeI, está más enfocada al suministro interno de TdeI con una orientación temporal en el presente, el Gobierno de las TdeI es más amplio, ya que además pretende atender las demandas externas (de los clientes, usuarios, entidades empresariales involucradas) en un horizonte temporal futuro".

Así mientras la gestión se centra en administrar e implementar las estrategias en el día a día, el gobierno se encarga de fijar dichas estrategias junto con la política y la cultura de la organización.

El Gobierno de TdeI, constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que las TdeI soporten y faciliten el desarrollo de los objetivos estratégicos definidos.

De acuerdo con Piattini [40], las TdeI deben de ser ágiles, ya que el alineamiento organizacional es uno de los desafíos más importantes a los que se enfrentan las organizaciones, y desafortunadamente las dificultades en conseguir y mantener un alineamiento estratégico no son correctamente valorados.

Hacemos una reflexión en este punto, en referencia al texto anterior y al enfoque del desarrollo del SGTI en el marco de una AEI.

Cualquier empresa es más y mayor que un sistema de información que gestione sus procesos, eso es indudable, cambia la perspectiva si la empresa es vista como un sistema, de acuerdo a lo señalado en el apartado 3.1.1, donde establecíamos las razones por las cuales desarrollar el SGTI bajo la visión de AEI.

El texto de referencia de Piattini, es totalmente el reflejo de la dinámica que existe en las organizaciones, donde podríamos decir que el alineamiento entre los objetivos del negocio (Arquitectura de negocios) y su soporte tecnológico para la gestión (Arquitectura de información) es momentáneo (quizás meses o pocos años).

Los esfuerzos para conservar y mantener el alineamiento son importantes en las organizaciones, la entropía organizacional que se genera por la dinámica propia de los negocios, las interrelaciones entre los diversos componentes de la organización y las entidades empresariales con las que tiene relación, obligan sobre la marcha a tomar medidas para mantenerla de no ser así los impactos en costos, calidad de los productos, niveles de servicio, satisfacción de los clientes se pueden ver seriamente afectados.

A la luz de lo anterior, y tomando en cuenta que el tema del gobierno de las organizaciones está atendido por el área del conocimiento del Gobierno Corporativo, que según la definición de la Organización para la Cooperación y el Desarrollo Economico (OCDE por sus siglas en inglés, Organization for Economic Co-operation and Deveploment)

> “Un conjunto de relaciones entre la dirección de las empresas, su consejo, sus accionistas y los terceros interesados. El Gobierno Corporativo también provee la estructura a través de la cual los objetivos de la sociedad son determinados, así como es monitoreado su desempeño y cumplimiento”,

resalta el beneficio de conceptualizar a la empresa como un sistema y configurarlo como una AEI.

La propuesta de Gobierno Corporativo está fuera del alcance de esta tesis, por tanto la propuesta del gobierno del SGTI la haremos bajo el enfoque y alcance de los estándares existentes de Gobierno de las TdeI. Donde el referente de la dinámica es la Arquitectura de negocios y las que hay que alinear son las Arquitecturas de información y tecnológica.

Tecnologías asociadas a la AEI, como la Arquitectura orientada a servicios (SOA por sus siglas en inglés) atienden el tema, donde los componentes reutilizables en toda la organización son los servicios, tecnológicamente conocidos como los web services.

El enunciado de Gobierno de TdeI garantiza que:

- Las TdeI estén alineadas con la estrategia del negocio,
- Los servicios y funciones de TdeI se proporcionan con el máximo valor posible o de la forma más eficiente y,
- Todos los riesgos relacionados con TdeI son conocidos y administrados y los recursos de TdeI están seguros

La adopción de un Gobierno de TdeI, implica establecer o adoptar un marco de referencia para que a través de sus métodos y prácticas permitan establecer:

- Criterios de información exigidos por los requisitos de negocio
- Procesos de negocio y,
- Recursos a utilizar

Las características de los marcos de referencia son:

- Están orientados a procesos, tanto de TdeI como del negocio
- Se debe definir el propietario del proceso, la responsabilidad sobre el proceso y la criticidad del mismo
- Están basados en prácticas comúnmente aceptadas, para aprovechar la experiencia del mercado y ofrecer un conjunto de medidas de control multinacional, evento especialmente importante para la auditoría

Siguiendo con Piattini [40], en general se pueden identificar cinco dominios principales de Gobierno de las TdeI que aplicaremos al SGTI, estos se describen en la tabla 40.

Tabla 40. Dominios del gobierno de tecnologías de la información

Dominio del Gobierno del SGTI	**Descripción**
Alineamiento estratégico del SGTI	Mantener alineadas las Arquitecturas de negocios, información y tecnológica
Entrega de valor del SGTI	Ejecutar la propuesta de valor a lo largo del ciclo de la cadena de valor de la empresa,

Dominio del Gobierno del SGTI	Descripción
	asegurando que el SGTI entregue los beneficios prometidos respecto a la estrategia, concentrándose en la optimización de los costos
Gestión de riesgos	Diseñar correctamente la administración de riesgos incluyendo en el sistema de gestión de la seguridad de la Información
Gestión de los recursos	Adoptando administración de recursos humanos y costos como se señala en administración de proyectos
Medición del desempeño	Diseñar y utilizar un cuadro de mando integral

En estas recomendaciones del Instituto de Gobierno, destacan los QUÉ y la parte medular son los CÓMO, ambos dominios se tienen que atender, bajo la compatibilidad de un marco de referencia.

En la tabla 41 se muestran el conjunto de acciones a realizar para implentar el gobierno del SGTI.

Tabla 41. Acciones a realizar para la implementacion del gobierno del SGTI

Actividades para la implementación según IGTI	Acciones para el SGTI
Establecer un marco de gobierno organizacional	Formar un Comité de gobierno con representantes de las entidades empresariales involucradas en el SGTI Establecer la normatividad que regule al Comité, así como las facultades sobre el SGTI Formular el Plan de anual de actividades
Alinear la estrategia del SGTI con los objetivos del negocio	Mantener actualizada la Arquitectura de negocios Mapear la Arquitectura de negocios hacia la Arquitectura de información
Entender/definir los riesgos	Diseñar, implementar y operar la administración de riesgos Diseñar, implementar y operar un sistema de gestión de la seguridad (ISO/IEC 27001)

Actividades para la implementación según IGTI	Acciones para el SGTI
Definir las áreas objetivo	Con base en las prioridades y jerarquías del negocio identificar las áreas de la Cadena de valor y soporte de la empresa, lo que se traduce en la fortaleza de la metodología es decir la ventaja competitiva
Analizar las capacidades actuales e identificar las brechas	Con base en la Administración de la demanda, la Administración de la capacidad, los procesos de mejora continua (ISO 9001:2008) de manera preventiva detectar las desviaciones de la empresa, así como proponer las medidas preventivas de contención
Desarrollar las estrategias de mejora	Con base en un sistema de gestión de la calidad (general ISO 9001:2008 o de TdeI ISO/IEC 20000:2005) establecer el Programa de mejora continua
Medir los resultados	Con base en el marco de referencia seleccionado establecer las métricas e indicadores de la gestión en todas las capas de la arquitectura.
Repetir los pasos anteriores de manera continúa	A través del programa de mejora continua realizar la evaluación y retroalimentación de la organización

Según el Instituto de Ingeniería del Software [W23] (SEI por sus siglas en inglés), se puede medir el nivel de madurez organizacional a partir del desarrollo evolutivo de sus procesos, la tabla 42 describe estos cinco niveles.

Tabla 42. Niveles de madurez organizacional según el SEI

Nivel de madurez	Descripción
Inexistente-0	No hay procesos reconocibles
Inicial-1	Se reconoce la necesidad de atender las actividades relacionadas con el proceso de las TdeI, pero no hay procesos estandarizados, dependen de iniciativas individuales y de la experiencia del equipo de gestión de las TdeI
Repetible-2	Intuitivo, se tienen prácticas regulares de gobierno como reuniones de revisión, creación de informes de desempeño, con la participación voluntaria de algunas

Nivel de madurez	Descripción
	entidades empresariales involucradas del negocio, no hay comunicación formal de procedimientos y la responsabilidad se deja a las personas
Definido-3	Se define un marco organizacional y de procesos para la gestión de las actividades de TdeI. Se institucionalizan las prácticas exitosas y las técnicas utilizadas son relativamente simples.
Gestionado y medible-4	Se desarrollan objetivos y las medidas de la mejora de los procesos de TdeI se entienden bien. Se comunican a la dirección resultados en forma de cuadro de mando integral. Se trabaja conjuntamente en el objetivo de maximizar el valor de las TdeI y la gestión de riesgos asociados con las TdeI.
Optimizado-5	Se desarrollan prácticas de gobierno de TdeI mediante aproximaciones sofisticadas utilizando técnicas efectivas y eficientes. Existe una verdadera transparencia de las actividades de las TdeI y la estrategia de TdeI está controlada. La práctica de la mejora continua de las TdeI se encuentra embebida en la cultura e incluye comparativos externos y auditorías independientes.

Son estándares de Gobierno de TdeI: ITIL, COBIT, ISO/IEC 38500.

ISO/IEC 38500 es un estándar publicado en Junio de 2008 en forma rápida, cuyo origen es la norma Australiana AS58015-2005 [R34].

La definición según ISO/IEC 38500 de Gobierno de TdeI [R32] y [R33] es la siguiente:

> "Es el sistema mediante el cual, se dirige y controla el uso actual y futuro de las TdeI. Incluye la evaluación y la dirección de planes para el uso de las TdeI en el soporte a la organización y la monitorización de este uso para el cumplimiento de los planes, así como la definición de estrategias y políticas relativas al uso de las TdeI en la organización".

El estándar se puede representar mediante una matriz en la cual las tareas para el gobierno se centran en: evaluar dirigir y monitorear, así como seis principios sobre los que se ejercen las tareas:

Principios	Evaluar	Dirigir	Monitorear
Responsabilidad			
Estrategia			

Principios	Evaluar	Dirigir	Monitorear
Adquisición			
Rendimiento			
Cumplimiento			
Factor humano			

Este estándar está orientado al buen uso de las TdeI.

COBIT en su Versión 4.1 (Control, Objetives for Information and Related Technology) es un estándar compuesto por 4 dominios y 34 objetivos de control. Los cuatro dominios son:

- Planear y organizar
- Adquirir e implementar
- Entregar y dar soporte
- Monitorear y evaluar

COBIT está orientado a la gestión de las TdeI.

En este punto, la disyuntiva de la selección de un marco de referencia para el Gobierno del SGTI, nos encontramos con un marco orientado al buen uso de los recursos de SGTI (ISO/IEC 38500 [R10]) y otro a la buena gestión (COBIT) de los recursos del SGTI.

Para el desarrollo de esta tesis, en especifico en el apartado de Gobierno del SGTI, la propuesta es emplear la plataforma compuesta por los estándares ISO 9001:2008, ISO/IEC 20000:2005, las prácticas de ITIL V3.0 e ISO/IEC 27001, que son compatibles, complementarias y están interrelacionadas.

El razonamiento para seleccionar esta plataforma de Gobierno del SGTI se fundamenta en lo siguiente:

Las TdeI son habilitadoras y están a disposición del negocio. El negocio está abstraído y conceptualizado mediante una Arquitectura de negocios. Los procesos de negocio son el motor e impulso de la empresa, en sus procesos y procedimientos se fundamenta el alcance de sus objetivos mediante estrategias.

El cliente está en el centro del diseño de las estrategias, sin clientes no hay negocio. En términos de lo anterior la satisfacción de los clientes es lo que le da la competitividad a la empresa. Se puede decir que la relación: objetivos del negocio-satisfacción de los clientes-mejora de los procesos y servicios-productos es lo que permite la existencia de las empresas.

El modelo de cadena de valor de Porter [6] para la competitividad, tiene su parte valiosa en descubrir los eslabones que le dan fortaleza a las empresas, es decir donde son fuertes y hacen que su competitividad sea más importante.

Por otra parte, como se ha mencionado con anterioridad la clave de la neutralización de la entropía organizativa, está en el alineamiento de las Arquitecturas de información y tecnológica con la Arquitectura de negocios. Ésta es la parte central de la solución.

El alineamiento no termina en un mapeo preciso y oportuno de los nuevos requerimientos o de los cambios a los requerimientos ya traducidos en especificaciones. La parte medular, está en cómo la empresa absorbe los cambios, como las personas los reciben, los aceptan, los entienden y como los ejecutan.

La herramienta que proporciona el estatus de esta capacidad de conversión organizativa son los indicadores, los cuales miden el nivel de madurez de la organización, el estándar ISO 9001:2008 considera parte integral la medición de la satisfacción de los clientes a partir de la medición de los objetivos, procesos, productos, servicios y de la mejora continua.

Otro factor clave, es que el SGTI es un impulsor, que pertenece a una industria con cultura de la calidad y la seguridad, sus procesos productivos están en ese contexto.

El sistema de gestión de la calidad (SGC) tiene como marco de referencia ISO 9001:2008, siendo el SGC auditable por segunda y tercera partes, además de que es certificable por organismo independiente, por lo que se requiere que el SGC esté permanentemente actualizado y mantenido, en otras palabras alineación entre los procesos documentados, con la ejecución de los mismos y evaluados a través de los clientes.

Otra ventaja, es que el marco de práctica de las normas ISO/IEC 20000:2005, ISO/IEC 27001 e ISO 9001:2008, tienen el enfoque del ciclo de Deming: planear, hacer, verificar y actuar.

Así también, el sistema de gestión de la calidad de las TdeI (SGTdeI) está soportado por el estándar ISO/IEC 20000:2005 y el sistema de gestión de la seguridad de la información (SGSI) está soportado por el estándar ISO/IEC 27001, ambos también son auditables y certificables por instancias independientes.

Por otra parte ISO/IEC 20000:2005 e ITIL V3.0 son complementarios, ya que ISO/IEC 20000:2005 está orientado a la organización e ITIL a la ejecución de los procesos de TdeI.

La norma ISO/IEC 27001 establece los lineamientos de los SGSI.

De acuerdo con Alberto G. Alexander [41], un SGSI se define como:

> "… el establecimiento de un sistema que determine que requiere ser protegido, y por qué, de qué debe ser protegido y cómo protegerlo".

ISO/IEC 27001 define la seguridad de la información como la

> "preservación de la confidencialidad, integridad, no repudio y confiabilidad".

De acuerdo a la norma ISO/IEC 27001 y sus anexos, los objetivos de control y controles son los siguientes:

- Política de seguridad
- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones
- Control de accesos
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Administración de incidentes de seguridad
- Administración de la continuidad del negocio
- Cumplimiento (legales, de estándares, técnicas y auditorias)

De los cuales podemos destacar la Administración de la continuidad del negocio, que de acuerdo a las mejores prácticas del ciclo de vida para el desarrollo y mantenimiento de un Plan de continuidad del negocio (PCN), se compone de las siguientes fases:

- Análisis de impacto del negocio
- Gestión del riesgo
- Desarrollo de estrategias de un PCN
- Desarrollo del plan de reanudación de operaciones
- Ensayo del PCN y,
- Mantenimiento del PCN

En congruencia con el nivel de madurez de la organización el SGSI, debe de proporcionar la mejora en la madurez de la seguridad de la organización, como lo establece Aceituno [5], la seguridad debe de ser reconocida como un proceso en el que se va evolucionando en términos de la implementación del SGSI del nivel 0 hasta alcanzar el nivel 5.

De esta forma ITIL V3.0 e ISO/IEC 27001 son compatibles, al ser la gestión de la seguridad un proceso de ITIL.

Finalmente el componente que permite la articulación entre estos estándares y que es un requisito que debe de cumplir un marco de referencia de Gobierno de las TdeI, es la forma de medir y presentar de manera integrada el nivel de madurez de la organización. Con este enfoque se cumple emplear el estado del arte de cada componente de la solución.

En términos de lo anterior, aunque la ortodoxia de gobierno de TdeI no contempla a la norma ISO 9001:2008, para los efectos de nuestro enfoque de AEI satisface nuestros requerimientos de gobierno del SGTI, al cumplir con la definición del IGTI, de ser gestor de las TdeI con un enfoque a clientes internos y externos con un horizonte temporal futuro avalado por las revisiones obligatorias de la alta dirección y, las auditoría internas y externas para la certificación.

El sistema de gestión de la calidad, el sistema de gestión de las TdeI y el sistema de gestión de la seguridad de la información, conforman cada uno una estructura documental piramidal, en donde el primer nivel es el de más detalle, siendo éste el que se encarga de llevar los registros de la operación del sistema de gestión y que otorga las evidencias para las revisiones y auditorias.

El nivel 2, proporciona las herramientas para el trabajo cotidiano, como son guias, instructivos, normas operativas y procedimientos de la operación. El nivel 3 proporciona la parte normativa con la que se gobierna a la organización y que reflejan el cumplimiento de cada apartado y cláusulas de los estándares que se aplican, finalmente el nivel 4 representa el manual de calidad, manual de seguridad de la información o el manual de gestión de TdeI, en el que están plasmadas, las políticas, el alcance, los objetivos, la matriz RACI, el modelado de los procesos y la normatividad que se tiene que cumplir.

La figura 61, muestra la pirámide documental de los sistemas de gestión de las normas ISO, plataforma del gobierno del SGTI.

En el tabla 43 se presenta una comparación y alcance de la plataforma propuesta para el gobierno del SGTI con respecto a COBIT 4.1.

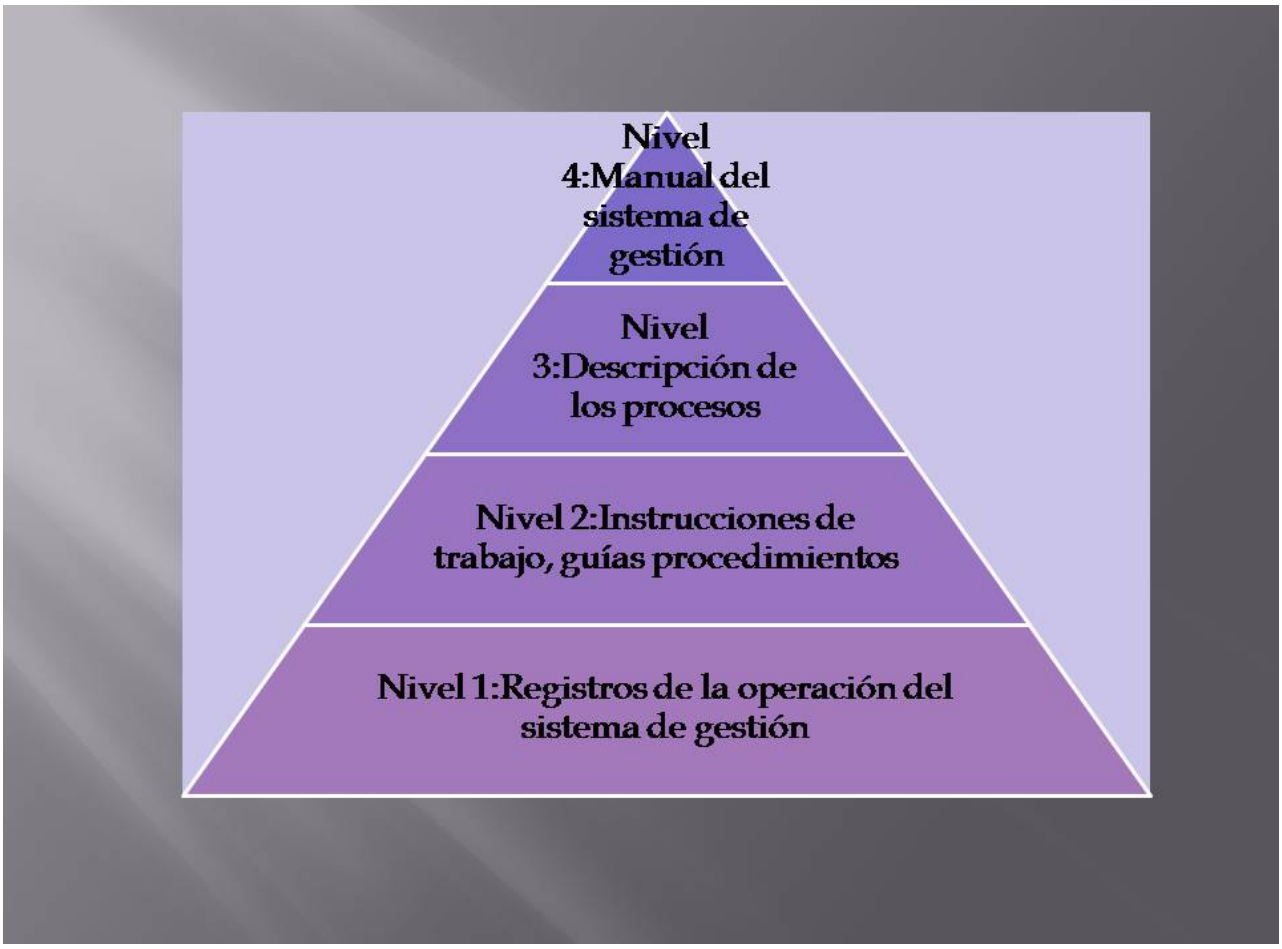


Figura 61. Pirámide documental de los sistemas de gestión soportados por las normas ISO 9001:2008, ISO/IEC 20000:2005 e ISO/IEC 27001

Tabla 43. Comparacion de plataforma de gobierno SGTI-COBIT 4.1

Dominios y procesos de COBIT 4.1	**Componente de la plataforma SGTI**	**Proceso o apartado del componente de la plataforma SGTI**
Planear y organizar		
P01 Definir el plan estratégico de TI	ISO 9001:2008	4.2.1 Generalidades del SGC 4.2.2 Manual de calidad 5.4 Planificación
P02 Definir la arquitectura de Información	Arquitectura empresarial de información (AEI)	Fase: Arquitecturas de negocios e información

Dominios y procesos de COBIT 4.1	Componente de la plataforma SGTI	Proceso o apartado del componente de la plataforma SGTI
P03 Determinar la dirección estratégica	ISO 9001:2008	5.4 Planificación
P04 Definir procesos, organización y relaciones de TI	ISO 9001:2008	4.2.2 Manual de calidad Arquitectura de negocios y su alineamiento con las arquitecturas de información y tecnológica
P05 Administrar la Inversión en TI	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	5.4 Planificación 3.1Responsabilidad de la dirección Administración financiera
P06 Comunicar las aspiraciones y la dirección de la gerencia	ISO 9001:2008	5 Responsabilidad de la dirección
P07 Administrar recursos humanos de TI	ISO 9001:2008 ISO/IEC 20000:2005	6 Gestión de recursos 6.2 Recursos humanos 6.4 Ambiente de trabajo 3.3 Competencia, conciencia y entrenamiento
P08 Administrar calidad	ISO 9001:2008	4.2.4 Manual de calidad
P09 Evaluar y Administrar riesgos de TI	ISO/IEC 20000:2005 ISO/IEC 27001 ITIL V3.0	6.6 Administración de la seguridad de la información 4 Sistema de gestión de la seguridad de la información Administración de la seguridad de la Información Administración de la continuidad de los servicios
P10 Administrar Proyectos	ISO 9001:2008	5.4 Planificación
Adquirir e implementar		
	ISO 9001:2008	7.1 Planificación del producto

Dominios y procesos de COBIT 4.1	Componente de la plataforma SGTI	Proceso o apartado del componente de la plataforma SGTI
AI1 Identificar soluciones automatizadas	ISO/IEC 20000:2005 ITIL V3.0	7.2 Procesos relacionados con el cliente 7.3 Diseño y desarrollo 4 Planificación e implementación de la gestión de servicios de TdeI 5 Planeación e implementación de nuevos y actualizados servicios de TdeI Administración del portafolio de servicios Administración de la demanda
AI2 Adquirir y mantener el software aplicativo	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	6 Gestión de recursos 6.3 Infraestrcutura 7.4 Compras 5 Planificación e implementación de nuevos y actualizados servicios de TdeI 10 Procesos de liberación de servicios Administración de los cambios Administración de la liberación y el despliegue Administración de proveedores
AI3 Adquirir y mantener la infraestructura tecnológica	ISO 9001:2008 ISO/IEC 20000	6 Gestión de recursos 6.3Infraestructura 7.4 Compras 7.6 Control de los dispositivos de seguimiento y medición 6 Entrega de servicios
AI4 Facilitar la operación y el	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	6.2 Recursos humanos 6.3 Infraestrcutura 6.4 Ambiente de trabajo 6 Entrega de servicios Administración de la disponibilidad Administración de la continuidad

Dominios y procesos de COBIT 4.1	Componente de la plataforma SGTI	Proceso o apartado del componente de la plataforma SGTI
uso		del servicio Administración de la capacidad Administración de la configuración
AI5 Adquirir recursos de TI	ISO 9001:2008	7.4 Compras
AI6 Administrar cambios	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	4.1Requisitos de la documentación 9 Procesos de Control Administración de los cambios
AI7 Instalar y acreditar soluciones y cambios	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	4.1Requisitos de la documentación 7.2Procesos relacionados con cliente-usuario 7.5Producción y prestación del producto-servicio 6 Procesos de entrega de servicios 9 Procesos de control Administración de cambios Administración de liberación y despliegue Administración de configuración y activos del servicio
Entregar y dar soporte		
DS1 Definir y administrar niveles de servicio	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	7.1 Planificación de la realización del producto-servicio 7.2 Procesos relacionados con el cliente-usuario 7.5 Producción y prestación del producto-servicio 6 Procesos de entrega de servicios Administración de diseño del servicio Administración de la operación Mejora continua
DS2	ISO 9001:2008	3 Procesos interrelacionados

Dominios y procesos de COBIT 4.1	Componente de la plataforma SGTI	Proceso o apartado del componente de la plataforma SGTI
Administrar servicios de terceros		7.1Provisión de recursos
	ISO/IEC 20000:2005	6 Procesos de entrega de servicios 7 Procesos de relaciones
	ITIL V3.0	Administración de la estrategia Administración del diseño de servicios Administracion de proveedores
DS3 Administrar desempeño y capacidad	ISO 9001:2008	8 Medición, análisis y mejora
	ISO/IEC 20000:2005	6 Procesos de entrega del servicio
	ITIL V3.0	Administración de la operación
DS4 Garantizar la continuidad del servicio	ISO 9001:2008	7.1Planificación de la realización del producto-servicio 7.2 Procesos relacionados con el cliente-usuario 7.5 Producción y prestación del producto-servicio
	ISO/IEC 20000:2005	6 Procesos de continuidad
	ITIL V3.0	Administración de la operación
DS5 Garantizar la seguridad de los sistemas	ISO 9001:2008	7.1Planificación de la realización del producto-servicio 7.2 Procesos relacionados con el cliente-usuario 7.5 Producción y prestación del producto-servicio
	ISO/IEC 20000:2005	6 Procesos de entrega de los servicios
	ISO/IEC 27001	SGSI
DS6 Identificar y asignar costos	ISO 9001:2008	3 Procesos interrelacionados
	ISO/IEC 20000:2005	6 Entrega de servicios
	ITIL V3.0	Administración de la estrategia
DS7	ISO 9001:2008	6.2 Recursos humanos

Dominios y procesos de COBIT 4.1	Componente de la plataforma SGTI	Proceso o apartado del componente de la plataforma SGTI
Educar y entrenar a los usuarios		
DS8 Administrar la mesa de servicio y los incidentes	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	7.2 Procesos relacionados con el cliente-usuario 7.5 Producción y prestación del producto-servicio 8 Procesos de solución Administración de la operación
DS9 Administrar la configuración	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	6.3 Infraestructura 9 Procesos de control Administración de la transición
DS10 Administrar los problemas	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0	3 Procesos interrelacionados 8 Procesos de solución Administración de la operación
DS11 Administrar los datos	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0 ISO/IEC 27001	6.3 Infraestructura 6 Proceso de entrega de servicio Administración de la transición Sistema de gestión de la seguridad SGSI
DS12 Administrar el ambiente físico	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0 ISO/IEC 27001	6.4 Ambiente de trabajo 6 Proceso de entrega del servicio 8 Procesos de control 10 Procesos de liberación Administración de la transición Administración de la operación Administración de los recursos
DS13	ISO 9001:2008	3 Procesos interrelacionados 7.2 Procesos relacionados con el cliente-usuario

Dominios y procesos de COBIT 4.1	Componente de la plataforma SGTI	Proceso o apartado del componente de la plataforma SGTI
Administrar las operaciones	ISO/IEC 20000:2005 ITIL V3.0	7.5 Producción y prestación del producto-servicio 8 Procesos de solución 9 Procesos de control 10 Procesos de liberación Administración de la operación
Monitorear y evaluar		
ME1 Monitorear y evaluar el desempeño de TI	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0 ISO/IEC 27001	8 Medición, análisis y mejora continua Mejora continua SGSI
ME2 Monitorear y evaluar el control interno	ISO 9001:2008	5.6 Revisiones por la dirección Auditorías internas y externas
ME3 Garantizar cumplimiento regulatorio	ISO 9001:2008	4 Sistema de GC
ME4 Proporcionar Gobierno de TI	ISO 9001:2008 ISO/IEC 20000:2005 ITIL V3.0 ISO/IEC 27001	Plataforma integrada ISO 9001:2008-ISO/IEC 20000:2005-ISO/IEC 27001-ITIL V3.0

La norma ISO/IEC 20000:2005 Gestión de Servicios de Tecnología de la Información (Information Technology Service Management) establece la plataforma en la organizaciones para la Administración de los servicios de TdeI, mientras que ITIL V3.0 reúne un conjunto de buenas prácticas para la gestión, desarrollo, despliegue y entrega de servicios de TdeI.

La norma ISO/IEC 20000:2005 cumple con el ciclo de vida de los procesos de calidad, es decir está estructurado y orientado a los procesos de:

- Planear, a través de la administración del plan de servicios

- Hacer, a través de la administración de la implementación del servicio y proporcionar los servicios
- Verificar, a través de monitorear, medir y revisar y,
- Actuar, a través de la mejora continua.

Un ejemplo de la relación entre los procesos del estándar ISO/IEC 20000:2005 y las prácticas recomendadas por ITIL V3.0, se muestra en la figura 62.

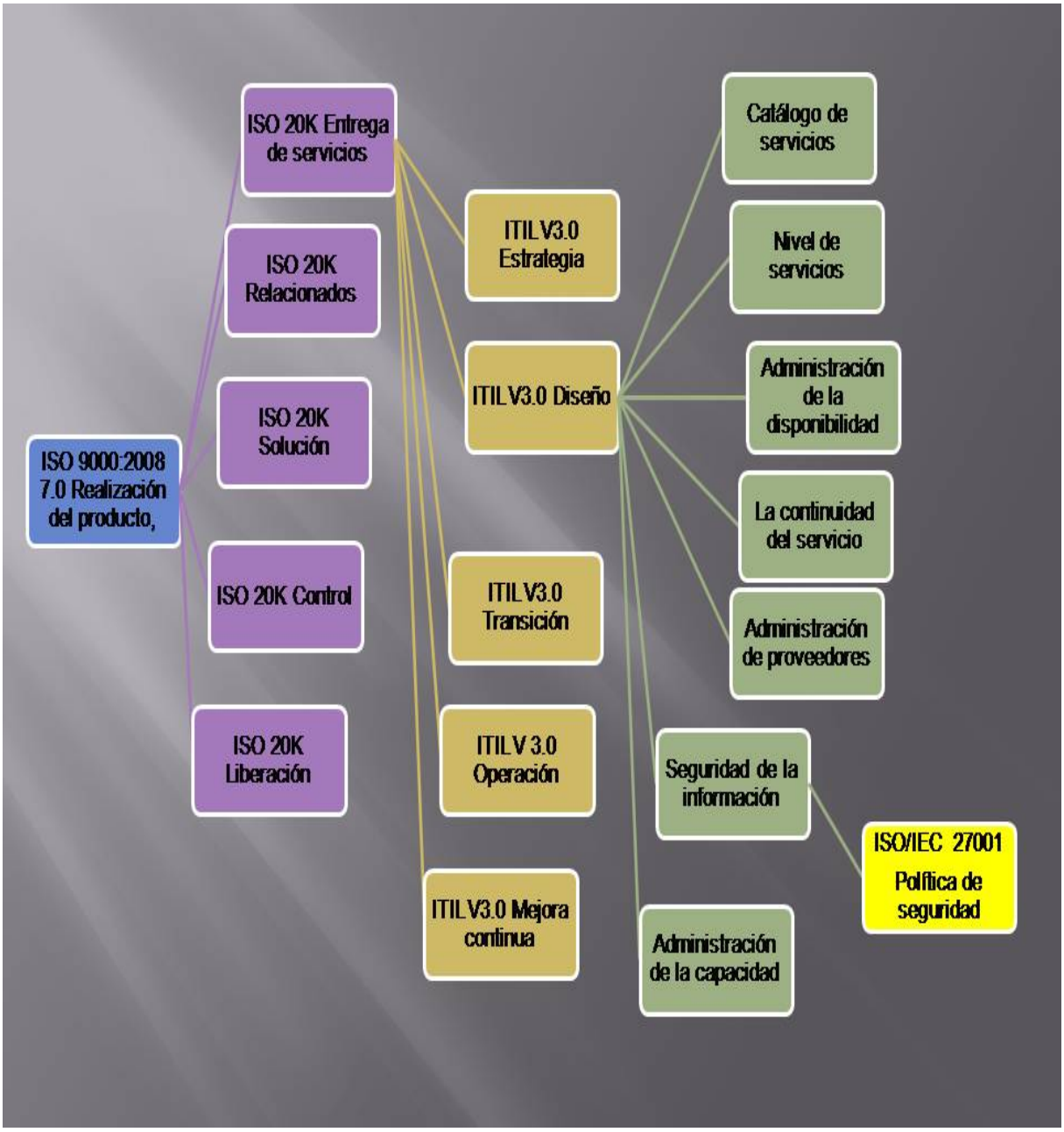


Figura 62. Correlación entre la norma ISO/IEC 20000:2005 e ITIL V3.0

Como lo especifica la norma ISO/IEC 20000:2005, la integración y estructura de los procesos aplicados al SGTI se muestran en la tabla 44.

Tabla 44. Procesos ISO/IEC 20000:2005 aplicados al SGTI

Procesos ISO/IEC 20000:2005	**Subprocesos**	**Aplicación al SGTI**
Liberación de servicios	Administración de niveles de servicio	Identificación, diseño y mantenimiento de los servicios a partir de las funcionalidades.
	Reporte de servicios	
	Administración de la continuidad y disponibilidad del servicio	Medidas predictivas y preventivas sobre el funcionamiento de los servicios críticos, en el entorno de las tarjetas con el SGTI
	Presupuesto y contabilidad de servicios de TI	Procesos del eslabón de la infraestructura organizacional
	Administración de la capacidad	Monitoreo sobre el comportamiento de la demanda del portafolio de perfiles de tarjetas y aplicaciones
	Administración de la seguridad de la información	De acuerdo al SGS mediante ISO/IEC 27001
Procesos relacionados	Administración de relaciones de negocio	Procesos de los eslabones de mercadotecnia y ventas
	Administración de	Mediante el comportamiento

Procesos ISO/IEC 20000:2005	Subprocesos	Aplicación al SGTI
	proveedores	de inventarios, niveles de servicio otorgados por terceras partes
Procesos de solución	Administración de incidentes	A través de mesa de ayuda
	Administración de problemas	A través de mesa de ayuda
Procesos de control	Administración de la configuración	Mantenimiento y actualización de acuerdo a los cambios que se realicen en los servicios en función de modificación a especificaciones al SGTI
	Administración de los cambios	Aplicación de las políticas del control de cambios
Procesos de liberación	Administración de la liberación	Los servicios que especifique el SGTI se puedan crear, instalarse, comprobarse e implementarse en paquetes de versiones exitosamente y dentro del plazo establecido

El gobierno del SGTI, aplica a las actividades permanentes del SGTI, es decir a la operación de todos los días, a cumplir con los niveles de servicio acordados, así como a mantener alineados los servicios de TdeI a la AEI, en este sentido, la adopción de la plataforma propuesta conlleva a la implementación de la Administración de operaciones de TI que de acuerdo a ITIL V3.0 sus objetivos son:

- Alcanzar la estabilidad de los procesos y actividades del día a día de la organización
- Inspeccionar y mejorar regularmente los servicios para ayudar a reducir costos a la vez que se mantiene la estabilidad de los mismos

- Aplicar las habilidades operacionales de forma oportuna para diagnosticas y resolver los fallos de las operaciones de TI

Los roles de la Administración de operaciones las podemos resumir en:

- Control de operaciones:
  - Supervisar la ejecución y monitorear las actividades operativas
  - Administración de consolas
  - Planificación de trabajos
  - Respaldo y restauración
  - Administración de impresiones
  - Mantenimiento

- Administración de instalaciones:
  - Administración del entorno físico, incluyendo centros de datos, sitios de recuperación y los equipos de energía y aire acondicionado relacionados
  - En su caso administración de contratos

De acuerdo a este entorno, las operaciones y las actividades relacionadas son medidas, la mejora continua proporciona las recomendaciones y los instrumentos necesarios para las partes interesadas a través de un mejor diseño, introducción y operación de los servicios, combinando principios, prácticas y métodos de gestión de la calidad, administración de cambios y mejora de la capacidad.
Los objetivos de la mejora continua los podemos resumir de la siguiente manera:

- Revisar, analizar y hacer recomendaciones sobre las oportunidades de mejora en cada fase del ciclo de vida
- Revisar y analizar los logros del nivel de servicio
- Identificar e implementar actividades para mejorar la calidad del servicio de TdeI, mejorando la eficiencia y la efectividad de los procesos de la administración de TdeI
- Mejorar la rentabilidad de la prestación de servicios de TdeI sin sacrificar la satisfacción del cliente
- Garantizar que los métodos aplicables de administración de calidad se utilizan para soportar las actividades de la mejora continua

La premisa, “se mejora lo que se controla, se controla lo que se mide”, es parte fundamental de los sistemas de gestión de la calidad y en especial los de la mejora continua. Existen dos visiones, la mejora de los procesos o la mejora de los productos.

Las razones para el monitoreo y medición en términos de la mejora continua son:

- Para validar las decisiones

- Para dirigir, fijar el orden de las actividades para alcanzar los objetivos establecidos
- Para justificar, presentar las pruebas necesarias para documentar las medidas recomendadas
- Para intervenir, identificar un punto de intervención

Los tipos de métricas para este contexto, pueden agruparse de la siguiente forma:

- De tecnología: Rendimientos, disponibilidad
- De procesos: Calidad, rendimiento, valor, cumplimiento madurez de la organización)
- De servicio: Disponibilidad, respuesta

De acuerdo con Oetringer [35] y Brooks [36], la mejora continua y el proceso de medición, a partir de métricas y sus indicadores correspondientes establecen la importancia de una Línea base por considerar que:

- Es un punto inicial o de referencia que permite que se hagan comparaciones posteriores
- Incorpora datos iníciales desde donde puede determinarse si se necesitan medidas o acciones para la mejora
- Que estén documentadas y asegurarse que se reconozcan y se acepten

Las medidas complementarias para el establecimiento de un Gobierno del SGTI son:

Dominios de gobierno según el I.T. Governance Institute	**ISO 9001**	**ISO/IEC 20000:2005**	**ITIL V3.0**	**ISO/IEC 27001**
Alineamiento estratégico del SGTI	Alineamiento con la Arquitectura de negocios: 4.1 Requisitos generales 4.2 Requisitos de la documentación 4.2.4 Manual de calidad 5 Responsabilidad de la Dirección 5.4 Planificación	3.1 Responsabilidad de la Administración 3.2 Requerimientos de la documentación 3.3 Competencia, conciencia y entrenamiento	Administración financiera Administración de la demanda Administración del portafolio de servicios Administración del catalogo de servicios Administración de los niveles de servicio Administración de la capacidad	5 Responsabilidades de la Administración 5.1 Comité de administración
Entrega de	5.6 Revisión por la Dirección 7.1 Planificación del producto 7.2 Procesos	4 Planificación e implementación de la Administración de servicios de TI 5 Planeación e	Administración de los cambios Administración de la liberación y el despliegue	7 Revisión del sistema de seguridad de la información

Dominios de gobierno según el I.T. Governance Institute	ISO 9001	ISO/IEC 20000:2005	ITIL V3.0	ISO/IEC 27001
valor del SGTI	relacionados con el cliente 7.3 Diseño y desarrollo 7.4 Compras 7.5 Producción y prestación del servicio 7.6 Control de los dispositivos de seguimiento y medición	implementación de nuevos y actualizados servicios de TI 6 Procesos de entrega de servicios 8 Procesos de solución 9 Procesos de control 10 Procesos de Liberación	Administración de eventos, incidentes y problemas	
Gestión de riesgos	5.4 Planificación	6.6 Administración de la seguridad de la Información 6.6.2 Identificación y clasificación de bienes de información 6.6.3 Prácticas de aseguramiento de riesgos de seguridad 6.6.4 Riesgos de bienes de información 6.6.5 Seguridad y disponibilidad de la información 6.6.6 Controles	Administración de la seguridad de la información Administración de la continuidad de los servicios Administración de la Disponibilidad	4 Sistema gestión de la seguridad de la información
Gestión de los recursos	6.1 Provisión de los recursos 6.2 Recursos humanos 6.3 infraestructura 6.4 Ambiente de trabajo	7. Procesos relacionados 7.2 Administración relacionada con el negocio 7.3 Administración de suministros	Administración de los suministros	5.2 Administración de recursos
Medición del desempeño	8 Medición, análisis y mejora 8.2 Seguimiento y medición 8.3 Control de Producto no conforme 8.4 Análisis de datos 8.5 Mejora	6.1 Administración de niveles de servicio 6.1.2 Acuerdos de niveles de servicio 6.1.3 Administración de procesos de niveles de servicio 6.1.4 Soporte de servicios acordados 7.2.3 Medición de satisfacción de clientes	Mejora continua	6. Auditorías internas 8 Mejora

La figura 63, muestra la estructura piramidal de la plataforma para el gobierno del SGTI, donde los tres niveles inferiores corresponden a los registros de la operación, los indicadores producto de la medición y al tablero de mando.

Figura 63. Estructura piramidal de la plataforma de gobierno del SGTI

4.4 Recomendaciones de un SGTI, como integrador de sistemas y ambientes de gestión en las organizaciones

La industria de las tarjetas inteligentes, involucra diversos perfiles de entidades empresariales participantes.

La división del trabajo, en ambientes de procesos centralizados o descentralizados a lo largo del ciclo de vida de la tarjeta inteligente, las responsabilidades y ámbitos de participación de los diversos actores está perfectamente delimitada, así como también los niveles de acceso y competencia para mantener la información actualizada.

La visión del SGTI como una herramienta de integración en el flujo de información que produce la operación cotidiana de un Programa de tarjetas inteligentes, lo podemos entender desde dos perspectivas, la seguridad y la integridad y eficacia de los procesos.

El activo más importante que se tiene en una tarjeta inteligente es la información contenida en ella. En los procesos productivos y en su operación en campo, están contempladas las técnicas de seguridad interna y externa, así como la gestión de la seguridad del ambiente del SGTI, pero puede suceder frecuentemente que la cadena se rompe por el eslabón más débil.

Este eslabón puede ser invisible para los involucrados, por tanto es necesario que un Programa de tarjetas inteligentes, sea diseñado, mantenido, actualizado y mejorado con los mismos niveles de seguridad a través de la toda la cadena de procesos y sistemas.

De acuerdo a la tabla 17 descrita en los apartado 3.6 y 3.7 de este trabajo, se tiene una visión de la relación del SGTI con otros sistemas de información, los cuales tienen una funcionalidad específica que es complementaria a la del SGTI en el contexto de un Programa de tarjetas y que por sus interfaces se transmite la información de los titulares de las tarjetas, sus transacciones electrónicas, los estados de los ciclos de vida, así como mensajería electrónica hacia/desde los puntos terminales de operación.

Cualquiera de estos puntos, pudiera ser en cualquier momento el eslabón más sensible.

La compatibilidad tecnológica entre los ambientes de los sistemas es importante, la compatibilidad entre las interfaces lógicas y físicas de los ambientes también es un tema que merece persistencia en su atención, por lo que hay que considerar que la compatibilidad y continuidad de los sistemas gestión de la seguridad de los ambientes y de la información contenida en ella es factor crítico de éxito para un Programa de tarjetas Inteligentes.

Normativamente se exigen las condiciones para disponer de ambientes seguros, normas específicas como EMV [W20] e ISO/IEC 27001 [W15] se implementan en ambientes de SGTI.

De acuerdo con lo anterior, el SGTI es el motor que recibe la información de las operaciones sobre tarjetas y aplicaciones, el impacto que tiene sobre el resto del ambiente es determinante, así como es determinante para toda la cadena de valor de los sistemas la seguridad del ambiente y de la información.

En la otra vertiente, es fundamental para un Programa de tarjetas inteligentes que la conceptualización, modelado e implementación del SGTI se realicé bajo un enfoque de AEI, que incorpore todas las visiones de los involucrados, facilite el alineamiento de los procesos de tecnología de la información con los procesos de negocio, evite los reprocesos no deseados de información, permita su mantenimiento sin tener impactos en los resultados de la operación cotidiana, mantenga los mismos niveles de calidad de la información, sea un habilitador de la

mejora continua y contribuya a reducir los costos de operación de las entidades empresariales.

Capítulo 5

Resultados, impacto y conclusiones

Resultados

La puesta en marcha de un programa de tarjetas inteligentes multiaplicativas requiere del soporte de un sistema de información que permita a los involucrados en el programa, disponer de información oportuna e integrada a través de los diferentes estados del ciclo de vida de las tarjetas inteligentes y sus aplicaciones.

En este sentido, a partir del objetivo de construir la especificación del estado del arte para la conceptualización, modelado e implementación de un sistema de información para la gestión de tarjetas inteligentes, se ha propuesto y desarrollado una metodología para poder integrar esta especificación.

El ambiente de operación de un programa de tarjetas inteligentes involucra a una diversidad de entidades empresariales multidisciplinarias y diferentes focos de negocio.

La participación de estas entidades empresariales, son parte importante en el ciclo de vida de las tarjetas, donde cada una de ellas juega un rol específico en tiempo y actividad.

En este entorno, el enfoque para la construcción de la especificación se ha realizado estudiando a las entidades empresariales como un sistema, de tal forma que la interacción entre ellas esté planificada, operada y gobernada como un todo, a partir de los diversos componentes que la integran.

En este sentido la definición de la especificación está basada en un enfoque de arquitectura empresarial de información (AEI), la cual ha permitido identificar cada uno de los componentes que forman las diversas arquitecturas, desarrollar los requerimientos de estos componentes y finalmente integrarlos para obtener la especificación completa del sistema.

El modelo referente para la construcción de la AEI está basado en el marco de TOGAF, el cual contempla tres capas de arquitectura (negocios, información y tecnológica) y procesos para la migración, la implementación y el gobierno del sistema.

Para la construcción de cada una de las diferentes arquitecturas que componen la AEI, se ha referido a las mejores prácticas, estándares y herramientas que se encuentren en el estado del arte de cada área del conocimiento en particular.

Por lo que, para la arquitectura de negocios, el modelado se ha obtenido a partir de la cadena de valor y de la cadena de soporte, el cual ha permitido plasmar y estudiar los procesos productivos e interrelaciones de las diferentes entidades empresariales.

La definición de los perfiles, especificaciones y características de los diversos componentes de las tarjetas inteligentes y sus aplicaciones, está basada en las

normas y los estándares publicados por los organismos de normalización ISO e IEC.

Como parte inherente a las especificaciones de los componentes de las tarjetas inteligentes como son los mecanismos de hardware y software para la seguridad se tienen referidas las especificaciones de los algoritmos y técnicas criptográficas de uso común en esta industria.

En cuanto a las especificaciones de las reglas de negocio de los procesos de gestión de tarjetas inteligentes en las diferentes etapas de preemisión, emisión y postemisión, los referentes empleados son los publicados por organismos como Global Platform y EMV, complementándolos con las definiciones y especificaciones para la arquitectura de tarjeta y dominios de seguridad de Multos y Java Card.

Estas especificaciones y funcionalidades han quedado expresadas en diccionarios.

El marco de referencia de AEI, establece que la capa de arquitectura de información está compuesta por la arquitectura de las aplicaciones y la arquitectura de datos. Estos dos componentes de la AEI están desarrollados como lo establecen los métodos de la Ingeniería de la información y de la Ingeniería del software. Los diferentes componentes de estas dos arquitecturas quedan expresados, mediante estructuras de datos, diagramas y diccionarios.

La arquitectura tecnológica está soportada por el modelo de referencia técnica de TOGAF, el cual involucra las diferentes capas de tecnología de hardware, software, interfaces, seguridad y calidad, necesarios para una correcta implementación del SGTI.

Adicionalmente, se incluyen en esta capa los componentes de infraestructura tecnológica obtenidos de la interrelación del SGTI con otros sistemas de información, las características propias del ambiente de operación centralizado o descentralizado, así como las capacidades y configuración necesarias de acuerdo a los niveles de servicio acordados y programas de continuidad del servicio requeridos.

La metodología presenta las etapas y procesos necesarios a desarrollar para la planeación de la migración al SGTI y la implementación del SGTI.

Se obtiene el cronograma y ruta crítica de las actividades de migración e implementación del SGTI.

Estos procesos son soportados por las mejores prácticas y estándares de la industria de las tecnologías de la información para el soporte y despliegue de servicios de tecnología de información, como son la norma ISO/IEC 20000:2005 (sistema de calidad de tecnologías de la información), ITIL V3.0 (Librería de

infraestructura de tecnología de la información) e ISO/IEC 27001 (sistema de gestión de la seguridad de la información).

Finalmente, el último componente de la especificación es la correspondiente a la etapa de operación del SGTI, la cual es estudiada bajo el enfoque del gobierno del SGTI.

Tomando como referencia las recomendaciones del Instituto de Gobierno de Tecnologías de la Información, la metodología propone una plataforma compuesta por los estándares ISO 9001:2008, ISO/IEC 20000:2005, ISO/IEC 27001 e ITIL V3.0 para llevar a cabo el gobierno del SGTI.

La razón principal de la propuesta de la plataforma de gobierno soportada por ISO 9001:2008, consiste en la visión de atender a las entidades empresariales como un sistema, en este entorno las entidades empresariales involucradas en el SGTI tienen una importante cultura organizacional, de calidad y de seguridad.

La medición y la mejora continua son parte importante de un marco de gobierno de TdeI, la correlación de las tres normas ISO, mencionadas anteriormente, con las mejores prácticas dadas por ITIL V3.0 permiten cumplir los preceptos enunciados por el Instituto de Gobierno de TdeI.

Así también, de acuerdo a la definición de estado del arte que adoptamos, destaca que se:

- Asume un conocimiento general del tema
- Enfatiza la clasificación de la literatura existente
- Evalúa las principales tendencias
- Desarrolla una perspectiva del tema
- Establece un tiempo de la investigación
- Señala los ámbitos y el alcance

Los resultados obtenidos en atención a este enfoque son:

Evaluación de las principales tendencias: En el mercado actualmente se percibe un incremento en la adopción de sistemas de gestión de tarjetas (SCMS por sus siglas en ingles Smart Cards Management Systems), así como también esfuerzos que se han venido concretando en la publicación de estándares relacionados con la interoperabilidad, como la norma ISO/IEC 24727 , promovida en su momento por la Administración General de Servicios de Estados Unidos (USA General Services Administration) a través de la especificación Government Smart Card Interoperability Specification (GSC-IS) V.2 (NISTR 6887) [W21].

Los beneficios que se prevé traerá consigo la publicación de esta norma, tanto en aspectos técnicos como de mercado, se señalan en el estudio de Giesecke & Devrient [R13] y [W30], entre los que destaca:

- Acceso de servicio de esquemas de alto nivel para desarrolladores de aplicaciones
- Llamadas opcionales de interfaces vía conexión de redes
- Unificación de mecanismos para diferentes tipos de tarjetas
- Framework de arquitectura de amplia cobertura y flexible

También Gemalto [R15] destaca los beneficios de la publicación de esta norma y su convergencia con normas europeas como la CEN prEN 15408.

En este sentido, como lo refiere Mike Hendry [R12], los dos principales contendientes en tarjetas multiaplicativas "abiertas" son Multos y Java Card.

> "Multos utiliza un estricto sistema de seguridad, donde cada aplicación es certificada por el emisor y por una Autoridad de administración global de llaves.
> Las aplicaciones son cargadas en forma cifrada y su descifrado ocurre hasta después de que la tarjeta verifica la aplicación del certificado. El SGTI, deberá trabajar con el emisor de la tarjeta, el desarrollador de la aplicación y la autoridad certificadora para producir y liberar las unidades de carga de la aplicación para la tarjeta.
> Java Card permite un amplio rango de opciones, Global Platform ofrece una combinación de ambientes de ejecución y especificaciones para soporte de sistemas que definen una carga segura de aplicaciones y procesos de administración de memoria. Es posible implementar Global Platform usando tarjetas Multos y sus procesos de carga".

Por tanto, el mercado espera que con la publicación y empleo de esta norma se mejore la interoperabilidad entre los diferentes proveedores, lo que conlleva a un ambiente de sistemas abiertos que impulsará el empleo de las tarjetas inteligentes con multiproveedores de aplicaciones impactando en la necesidad de utilizar sistemas de gestión de tarjetas inteligentes.

Por otra parte con un enfoque de mercado, en el estudio de investigación de Frost Sullivan [R14], señala que el factor clave para la extensión de los SGTI es la expansión de las tarjetas multiaplicaciones. La mayor parte de las tarjetas inteligentes actualmente cae en el sector de las tarjetas de identificación, seguidas por las de la banca y el gobierno. Extendiendo su potencial hacia las universidades, las de programas de lealtad y las del sector salud.

En esa medida la penetración del SGTI se vuelve una necesidad, que se ve acompañada de las facilidades de la mercadotecnia uno a uno.

Uno de los procesos claves de la expansión de las tarjetas inteligentes y por tanto de los SGTI, es la capacidad del proceso de actualización y mantenimiento en la etapa de postemisión, lo que debe de permitir la reutilización de espacios de memoria en la tarjeta de aplicaciones que hayan cumplido su vigencia, pudiendo

ser reutilizado con nuevas aplicaciones y con esto reducir los costos de manera importante.

Esto sin embargo conlleva procesos de coordinación en la cadena de negocios y tecnología preparada para la interoperabilidad.

Un detonante potencial son las especificaciones EMV, en la medida que este tipo de tarjetas crezca, la implementación de los SGTI serán sólo una consecuencia de la necesidad de gestión de cantidades importantes de tarjetas con aplicaciones que administren importantes valores como contenidos de las tarjetas.

Por tanto, de acuerdo a las tendencias actuales y futuras que se preveen por especialistas en el mercado de las tarjetas inteligentes, es recomendable que el levantamiento de las especificaciones para la implementación de un SGTI en el ámbito de un programa de tarjetas sea realizado bajo un enfoque de AEI, puesto qué facilitará la integración de los diccionarios de: perfiles de tarjetas, de perfiles de aplicaciones, la descripción de los estados del ciclo de vida de las tarjetas y de las aplicaciones y, la descripción de los procesos de gestión en un ambiente de interoperabilidad de plataformas de tarjetas inteligentes.

Desarrollo de una perspectiva del tema: Este trabajo integró diversas técnicas, métodos, enfoques, prácticas, normas y estándares para describir las especificaciones de un sistema de información.

El desarrollo de la especificación tiene dos vertientes:

- Emplear herramientas que estén en el estado del arte del área del conocimiento y,
- Que los entregables de las herramientas sean modulares, adaptables al tamaño y tipo de organización y; que la usabilidad otorgue condiciones de facilidad y flexibilidad para su mantenimiento y actualización

El soporte documental, metodológico y de contenidos de las especificaciones desarrolladas es la siguiente:

Marco de referencia	**Componentes**
Ingeniería de sistemas: Ingeniería de negocios	Orientado a procesos Orientado a producto
Arquitectura empresarial de información TOGAF	Arquitectura de negocios Arquitectura de aplicaciones Arquitectura de datos Arquitectura tecnológica Procesos de planeación de la migración e implementación

Marco de referencia	Componentes
	del SGTI Gobierno del SGTI
Cadena de valor	Modelo de análisis de negocio Actividades primarias de la organización Actividades de soporte
Ingeniería de la información	Modelado de datos Estructura de la Arquitectura de aplicaciones
Normas ISO e IEC	Especificaciones de tarjetas inteligentes
Global Platform	Especificaciones de procesos asociados con las tarjetas inteligentes
ISO/IEC 20000:2005	Administración de procesos de gestión de servicios de TdeI
ITIL V3.0	Gestión y entrega de servicios de TdeI
ISO 9001:2008	Gestión de la calidad
TQdM	Gestión de calidad de datos
ISO/IEC 27001	Gestión de la seguridad de la información
Administración de proyectos	Administración de proyectos

En un plano comparativo entre el enfoque del desarrollo de las especificaciones de conceptualización, modelado e implementación del SGTI con respecto a un enfoque tradicional de sistemas de información, podríamos destacar lo siguiente:

El énfasis fue puesto en abstraer a la empresa (en realidad conjunto de empresas) como un sistema, facilidad obtenida al emplear la metodología propuesta por E. Michael Porter, la cual es una herramienta orientada hacia el análisis de la ventaja competitiva de las organizaciones, y que en nuestro caso nos ha permitido organizar los procesos de manera natural como sucede para cualquier tipo de industria.

En segundo término y de acuerdo con el concepto empresa-sistema, emplear un marco de referencia que ponga a las reglas del negocio como el impulsor y a la tecnología como el habilitador, en este sentido, las metas y objetivos no solamente son las de TdeI, sino el alineamiento entre las arquitecturas habilitadoras (información y tecnológica) con la de negocios, por considerar que se obtiene este efecto, además de poder administrar en cierta forma la entropía organizativa seleccionamos un marco de arquitectura de empresarial de información.

Finalmente, proponer una plataforma de gobierno del SGTI (concebido como empresa-sistema), en el que se conjuguen los estándares y mejores prácticas de los procesos de negocio (ISO 9001:2008), con las ventajas que conlleva en la práctica disponer de procesos y procedimientos documentados, tablero de mando

para la medición de indicadores, gestión del clima laboral, la rastreabilidad de los procesos y su mejora continua, con las de TdeI (ISO/IEC 20000:2005, ISO/IEC 27001 e ITIL V3.0) las cuales potencian a la organización al mejorar la eficacia de los servicios de TdeI.

De acuerdo a lo anterior, los resultados en esta vertiente son el haber podido aprovechar las diferentes herramientas existentes tanto de la industria de las tarjetas inteligentes y de las TdeI para obtener una especificación integral de lo necesario para la implementación de un SGTI.

Impacto

Poder establecer de manera metodológica la integración de la diversidad de componentes necesarios para la determinación de los requerimientos de un sistema de gestión de tarjetas inteligentes, desde su etapa de conceptualización hasta la de su gobierno, es el objetivo principal de este trabajo.

En un programa de tarjetas inteligentes, existe una participación de diferentes entidades empresariales, de diferentes focos de negocio, así como diversos proveedores de diferentes áreas de conocimiento, cada uno de los cuales tiene un rol en un tiempo determinado.

El ciclo de vida de una tarjeta inteligente y de las aplicaciones que se almacenan en ella para posterior ejecución, son los procesos sobre los que gira la gestión de las tarjetas inteligentes.

El ambiente de operación centralizada o descentralizada establece condiciones importantes sobre las especificaciones del SGTI.

Los requisitos de calidad y seguridad del entorno de un programa de tarjetas son premisas que se deben de cumplir en términos de normas establecidas y especificaciones de las relaciones de servicio.

En el ambiente de la operación de los programas de tarjeta inteligente, existen otros sistemas de información con los que se tiene interfaz física y de comunicación de datos.

Bajo este contexto, el enfoque de AEI establece condiciones de integralidad para el buen gobierno del SGTI, que impacta directamente al gobierno de la empresa.

Como se refirió en el apartado de gobierno de TdeI, éste es sólo un componente de lo que se conoce como gobierno corporativo. Los marcos de referencia con los cuales se implementa, establecen los niveles de madurez que tiene una organización (niveles del 1 al 5 inicial, repetido, definido, gestionado y optimizado).

El mejor nivel organizacional sólo se logra en la medida que la planeación, la ejecución y los resultados están cada vez mejor estructurados, integrados y sistematizados. La adopción de mejores prácticas y diversos sistemas de gestión

no garantizan que este nivel organizacional mejore, está inmerso en este largo proceso de mejora de las organizaciones la participación y compromiso de la gente.

Pero también es innegable que se deben de disponer de herramientas adaptables y adoptables en cada organización.

Nuestra propuesta incorpora diferentes herramientas y metodologías, todas medibles, con el propósito de contribuir a la mejora organizacional desde esta posición.

Estos niveles de madurez de las organizaciones reflejan la cultura organizacional, y corresponden a procesos evolutivos, la experiencia demuestra que sólo las organizaciones que implementan sus procesos de negocio con el alineamiento correcto de la tecnología podrán aspirar a escalar estos niveles, haciéndolas más competitivas.

Por tanto en la metodología propuesta para la conceptualización, modelado, implementación de un sistema para la gestión de tarjetas inteligentes y el gobierno del mismo, está inmerso, a través de la implementación de los procesos de mejora continua, una propuesta de las formas de alcanzar mejores niveles de cultura organizacional. Éste es el impacto al que se aspira con este enfoque y metodología.

Conclusiones

Con respecto al estado del arte

Están incorporados en este trabajo para las vertientes de estudio que la componen los resultados de los últimos avances, en materia de tarjetas y su sistema de gestión, se han incluido las bases y propuestas normativas que rigen en la actualidad.

En materia de sistemas de información está referido el modelo de arquitecturas empresariales lo que le da profundidad y consistencia al estudio de los requerimientos de negocio vinculados con las especificaciones de sistemas, proporcionando las herramientas y facilidad de interrelacionar todos los componentes de una empresa.

En materia de entrega, despliegue y liberación de servicios de tecnología de información están incluidas las mejores prácticas y estándares actuales.

El empleo de estas herramientas posibilita que el ciclo de vida del SGTI tenga mayor tiempo de vigencia, se facilite su actualización, mantenimiento y mejora de manera integral y que los impactos por el mundo cambiante de los negocios en el SGTI puedan ser controlados y alineados sin generar caos organizacional.

Con respecto al aporte teórico y la técnica empleada

El aporte teórico, en primer término es el de poder disponer en un solo documento información actualizada de diferentes temas, identificar sus puntos de contacto y que a través de su integración potenciar el todo y cada uno de ellos.

También se logró la combinación e integración de los modelos, metodologías y estándares, aplicándolos a un área del conocimiento especializada, compleja y de alto nivel de dependencia en procesos, prácticas y tecnología.

Con estas consideraciones, el esfuerzo desplegado produjo una especificación funcional prototipo, y que de acuerdo al alcance y perfil de una empresa se pueda llevar a la práctica.

Con respecto a la técnica, empleada, integramos y resumimos los conceptos más importantes de las tarjetas inteligentes que nos permitieran abstraer y conceptualizar las reglas de negocio del SGTI, así también se expuso y se personalizó para este caso los principios de los estándares y herramientas que permitan realizar una implementación exitosa.

La aportación práctica

Adoptar diferentes marcos de referencia de diversas áreas del conocimiento y darles un sentido de utilización de acuerdo a los elementos objetivos que se disponen para diseñar de manera flexible y modular la adopción, desarrollo a la medida o contratación con un tercero de un SGTI.

Sin pretender ser una guía de adquisición o contratación, haber presentado el panorama de las industrias que están involucradas, los roles, sus responsabilidades y sus entregables, de tal forma que en el enfrentamiento de un proyecto similar se cuente con los elementos para conocer qué perfiles de entidades empresariales tienen que ser incorporadas en cualquiera de los escenarios viables posibles para implementar un SGTI, el cual puede ser desarrollado por un tercero o adquirir y parametrizar un producto existente en el mercado.

El caso de estudio, qué beneficios se obtuvieron

Integrar en un solo repositorio de contenidos la información necesaria para contemplar integralmente desde la conceptualización hasta la implementación y el gobierno un sistema de información de estas características.

Los objetivos

Se alcanzaron, al lograr en primera instancia documentar cada uno de los componentes con un grado de actualización suficiente y, posteriormente encadenarlos y poder utilizarlos en forma práctica para documentarlos y establecer un modelo con sus propias características.

Futuros trabajos, lo que está fuera de la investigación y del alcance

Quedaron fuera del alcance temas de la tecnología de las tarjetas, como el desarrollo del ciclo de vida de las aplicaciones, ejemplos típicos de multiaplicaciones, la conformidad EAL o ITSEC de los niveles de seguridad de la plataforma de las tarjetas inteligentes, y fuera de la investigación un comparativo de los SGTI que existen en el mercado.

Los trabajos futuros sobre el tema tendrán que girar en torno a profundizar en las especificaciones sobre los sistemas de información con los cuales el SGTI tiene interface. Por mencionar algunos de ellos que resultan fundamentales, son el sistema recolector de las transacciones electrónicas y los sistemas de administración de llaves, incluyendo el módulo de hardware seguro.

Recomendaciones

El desarrollo de proyectos de sistemas de información de alto impacto donde el nivel de integralidad sea parte fundamental para su éxito, es recomendable que su enfoque sea sistémico, contemplando y dándole prioridad a la arquitectura del negocio, utilizando las herramientas que faciliten su análisis, diseño, construcción, implementación y gobierno.

Las normas, estándares y prácticas están en permanente evolución, su selección y adopción tiene que ser cuidadosa a la vez que práctica y funcional.

El monitoreo y seguimiento de ellas conllevará a seleccionar las plataformas adecuadas para desarrollar, soportar y mantener los proyectos de sistemas.

Un SGTI es un sistema grande (en varios sentidos de la expresión) y de alto impacto, involucra industrias especializadas, diversas entidades empresariales, que maneja intrínsecamente importantes valores (monetarios, de información y de identidad de las personas), pero lo más importante es que su operación en campo es llevada a cabo por usuarios y clientes con diversa cultura de procesos y de sistemas e infraestructura tecnológica a distancia.

Bajo estas premisas, ningún esfuerzo en la planeación, diseño y operación de un sistema de estas características está de más, es decir, el camino del éxito para un

SGTI, inicia desde la correcta selección de las herramientas, pasando por el rigor y disciplina de su adopción y ejecución hasta el ejercicio cotidiano de la mejora continua.

En tal sentido, además del aporte académico del estado de arte, los sistemas de misión crítica o sistemas tipo SGTI tienen que ser valorados y evaluados como la empresa misma.

Lista de Figuras

Lista de Tablas

Lista de Diccionarios

Bibliografía

[5] Aceituno Canal, V. (2007). *Seguridad de la Información.* México, D.F.: Limusa, 1a edición.

[41] Alexander, A. G. (2007). *Diseño de un sistema de gestión de seguridad de información.* Colombia: Alfaomega, (R1, 2000)1a edición.

[7] Austin, T. (2001). *PKI.* USA: Wiley, first edition.

[36] Brooks, P. (2006). *(ITSM) Metrics for IT service management.* Wilco Amersfoort Netherlands: Van Haren Publishing, firts edition.

[15] Chamoun Nicolás, j. Y. (2006). *Administración Profesional de Proyectos La guía.* México, D.F.: Mc Graw Hill, 1a edición.

[12] Chen, Z. (2004). *Java Card Technology for Smart Cards.* USA: Addison Wesley, firts edition.

[11] Cook, M. A. (1996). *Building Enterprise Information Architectures.* New Jersey, USA: Prentice Hall, 1a edition.

[44] Corona Funes, R. (1998). *Estrategia, el cambio en la proyección del pensamiento empresarial.* México, D.F.: SICCO, 1a edición.

[1] Daltabuit Godás, E., Hernández Audelo, L., Mallén Fulerton, G., & Vázquez Gómez, J. d. (2007). *La Seguridad de la Información.* México, D.F.: Limusa, 1a edición.

[31] Date, C. J. *Introducción a los Sistemas de Bases de Datos.* Prentice Hall, .

[33] Davenport, T. H. (1999). *Ecología de la Información.* México, D.F.: Oxford, 1a edición.

[26] Elmaski, & Navathe. *Data Base systems.* Addison Wesley, .

[30] English, L. (1999). *Improving Data Warehouse and Bussiness Quality.* USA: Wiley, first edition.

[13] Gane, C., & Sarson, T. (1979). *Structured Systems Analysis.* USA: Prentice Hall, first edition.

[16] Gido, J., & Clements, J. P. *Administración éxitosa de proyectos.* Thomson, .

[39] Gómez Vieites, A. (2007). *Enciclopedia de la seguridad informática.* México, D.F.: Alfaomega Ra-Ma, 1a edición.

[14] Gray, C. F., & Larson, E. W. (2009). *Administración de proyectos.* Méico, D.F.: Mc Graw Hill, 4a edición.

[20] Haghiri, Y., & Torantino, T. *Smart Card manufacturing a practical guide.* Wiley, .

[43] Hares, J. S. (1992). *Information Engineering for the advanced practitioner.* England: Wiley, first edition.

[19]Hendry, M. (2007). *Multi application smart cards technology and application .* USA: Cambridge, first edition.

[22] Hendry, M. *Smart Card security and applications.* Artech House.

[37] Hopcroft, J. E., Motwani, R., & Ullman, J. D. (2002). *Introducción a la teoría de autómatas, lenguajes y computación.* España: Addison Wesley, 2a edición.

[34] Jalote, P. (2002). *CMM in Practice.* USA: Addison Wesley, 4th edition.

[21] Jurguensen, T. M. *Smart Cards developpers Toolkit.* Prentice Hall, .

[10] Kendall, K. E., & Kendall, J. E. (1997). *Análisis y Diseño de Sistemas.* México, D.F.: Prentice Hall, 3a edición.

[24] Lee, H. K., & R., W. *Quality information and knowledge .* Prentice Hall, .

[28] Lee, P. L., & R., Y. W. *Data quality Assesment communication of ACM.*

[27] Lee, S. D., & R. Y., W. *Data quality in context communication of the ACM.*

[38] Maiorano, A. H. (2009). *Criptografía técnicas de desarrollo para profesionales.* México, D.F.: Alfaomega, 1a edición.

[45] Morrisey, G. L. (1995). *Pensamiento estratégico, planeación a largo plazo, planeación táctica.* Prentice Hall Pearson .

[42] Mylls, R. (1994). *Information Engineering Case practices and techniques.* USA: Wiley, first edition.

[35] Oetringer, E. *The I.T. Strategy Management Process.* Van Haren Publishing.

[4] Perks, C., & Beveridge, T. (2003). *Guide to Enterprise IT Architecture .* U.S.A.: Springer-Verlag, first edition.

[8] Piattini Velthuis, M. G., García Rubio, F. O., & Caballero Muñoz-Reja, I. (2007). *Calidad de Sistemas Informáticos.* México, D.F.: Alfaomega Ra-Ma, 1a edición.

[40] Piattini Velthuis, M., & Hervada Vidal, F. (2007). *Gobierno de las tecnologías y los sistemas de información.* España: Ra-Ma, 1a edición.

[6] Porter, M. E. (2004). *Ventaja Competitiva.* México, D.F.: CECSA, 2a edición.

[3] Pressman, R. S. (2007). *Ingeniería del Software un enfoque práctico.* México, D.F.: Mc Graw Hill, 6a edición.

[18] Rankl, W. (2007). *Smart Card Applications design models for using and programming smart cards.* England: Wiley, first edition.

[17] Rankl, W., & Effing, W. (2007). *Smart Card Handbook.* England: Wiley, 3th edition.

[9] Sommerville, I. (2001). *Software Engineering.* USA: Addison Wesley, 6th edition.

[2] Tapiador Mateos, M., & Sigüenza Pizarro, J. A. (2005). *Tecnologías biométricas aplicadas a la seguridad.* México, D.F.: Alfaomega Ra-Ma, 1a edición.

[25] S., K. *Evaluating the quality of entity relationship models.* Journal of objects technology.

[32] Zahran, S. (1998). *Software process improvement.* England: Addison Wesley, first edition

Referencias

[R1] Recommended Practice for Architectural Description of Software-Intensive Systems. IEEE Standard 1471-2000

[R2] Government Smart Cards Handbook, G.S.A. USA General Services Administration

[R3] Standards ISO/IEC, International Standardization Organization/International Electrical Commite

[R4] Comparation of the top four Enterprise Architecture Methodologies, Rogers Sessiones

[R5] Smart Card: The Global Information Passport, Jack M Kaplane

[R6] Smart Card Forum Standard and Specifications of Smart Card An Overview

[R7] Identification cards, integrated circuits card Part 13. Commands for application management in multi application ISO/IEC JTC1/SC 17WG4 ISO/IEC 7816-13, ISO/IEC, Documento Draft

[R8] Estándares Tecnológicos, National Institute Standard of Technology (NIST)

[R9] ICT Security and Governance at the Ukho, Andy Porter, Head of IT Security and Governance:2008

[R10] ISO/IEC 38500 y el buen Gobierno de T.I, Beatriz Candano (CISM)

[R11] Procesos de Tecnología orientados a garantizar mejores resultados al negocio (Marzo 2008), Contact Summit

[R12] Smart Card management systems an overview, Mike Hendry

[R13] ISO/IEC 24727 A future standard for smart cards middleware, Stephen Spitz-Jens urmann-Gisela Meister, Geisecke&Devriant

[R14] Smart cards, Investigación de mercados de Sistemas de Gestión, Frost&Sullivan, El Mundo

[R15] Smart card Workshop 2007 Europeans Citizen Card and ISO/IEC 25727 Covergence, Gemalto

[R16] Java Card y Global Platform Disponible en www.grintain.com, Edgar Renteria Morales, Grupo de Investigación en tarjetas inteligentes (GRINTAIN) Universidad Autónoma de Baja california, Facultad de Ingeniería, Instituto de Ingeniería 2006

[R17] Arquitectura de Empresa, Visión General, Llanos Cuenca, Angel Ortiz
Andres Boza, IX Congreso de Ingeniería Organizacional, Gijon Sept. 2005
Centro de investigación Gestión en Ing. De Producción, Universidad de Valencia

[R18] ISO/IEC 15704, Requeriments for Enterprise Referente Architecture and Methodologies

[R19] Enterprise Modeling and Integration. Principle and applications, Vernadat, Chapman & Hall

[R20] Smart Policy and Administrative Guides, GSA Estados Unidos Octubre 2002

[R21] A Multi card Architecture for Smart Card Management Systems, Ryu Taro Toji y Yoshinori Wada, NTT Information Sharing Platform Laboratories Japon

[R22] Development Kit User Guide Java card 3 Platform V3.02 Connected and Classic edition, Sun Micro systems

[R23] Criptosistemas informáticos, Death Master
[R24] National Smart Card Framework, Marco de referencia del Gobierno de Australia, Gobierno de Australia
[R25] Australian Government Interoperability Frameworks, Marco de referencia de interoperabilidad, Gobierno de Australia
[R26] Smart Card Project design guide, Guía para el proyecto tarjetas Inteligentes, Gobierno de Australia
[R27] Diseño con microprocesadores basado en diagramas de estado, Leopoldo Silva Bijit, Universidad Técnica Federico Santa María Departamento de Electrónica
[R28] Card Specifications, Global Platform
[R29] SCMS Functional requeriments, Global Platform
[R30] Key Management Systems, Global Platform
[R31] Enterprise Architecture: A Governance Framework, Infosys
[R32] ISO/IEC 38500 The Corporate Governance of IT, www.isaca-london.org
[R33] ISO/IEC 38500, la norma por el Buen Gobierno de TI , Manuel Ballester Normas y Estándares
[R34] AS8015-2005, Australian Standard for Corporate Government IT
[R35] Documenting a catalog of Viewpoints to Describe the execution Architecture of a large software intensive systems for ISO/IEC 42010 Standard, Trosky B. Callo Arias, Paris Avgeriou Department of Mathematics and Computing Science University of Groningen The Netherlands Pierre America Philips Research and Embedded Systems Institute The Netherlands
[R36] IT Governance Executive Summary, IT Governance Institute

Mesografía

[W1] Algoritmos de cifrado, http://www.uaem.mx/posgrado/mcruz/cursos/optimizacion/problemas.pdf
[W2] Algoritmo AES, http://csrc.nist.gov/publications/fips197/fips-197.pdf
[W3] Algoritmo DES, http://csrc.nist.gov/publications/fips46-3/fips46-3.pdf
[W4] Algoritmo 3DES, http:csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
[W5] Arquitectura Empresarial de Información, www.objectwatch.com
[W6] Integración de TOGAF e ITIL, http://www.acis.org.co/fileadmin/Conferencias/IntegracionTOGAFeITIL.pdf
[W7] Especificaciones Global Platform,http:// www.globalplatform.org
[W8] Especificaciones Java card, http://www.java.sun.com/java.card
[W9] Metodología MIT Calidad de datos, http://web.mit.edu/tdqm
[W10] AEI TOGAF, http://www.togaf.com
[W11] Instituto de Gobierno de TI, htpp://www.itgi.org
[W12] Estado del arte, http://dis.unal.edu.co/~fgonza/courses/2005-II/seminario/estadoArte.pdf
[W13] Sistema de Información, www.websters-online-diccionary.org/definitions/systems
[W14] ITIL, http:///www.itil-officialsite.com/home/home.asp
[W15] Normas ISO/IEC, http://www.iso.org
[W16] Arquitectura FEA, http://www.whitehouse.gov/omb/e-gov/fea
[W18] AEI ZACHMAN, http://zachman.org
[W19] Algoritmo DES, http://tierradelazaro.com/public/libros/des.pdf
[W20] Normas EMV, http://www.emvco.com
[W21] Interoperabilidad GSA NIST, http://smartcard@nist.gov
[W22] Gobierno de TI COBIT, http://www.isaca.org.org
[W23] Modelos de Capacidades de Madurez CMMi, http://www.isaca.org.org
[W24] Microprocesadores ST, http://www.st.com
[W25] Infineon Microprocesadores, http://www.infineon.com
[W26] Micro controladores atmel, http://www.atmel.com
[W27] Microcontroladores renesas, http://www.america.renesas.com
[W28] Microprocesadores Phillips, http://www.phillipsind.com
[W29] Plataforma Multos, http://www.multos.com
[W30] Giesecke & Dreviant, http://www.gi-de.com
[W31] Frameworks Comparison and Correspondence for three archetypes,
[W32] Smart Card Alliance, http://www.smartcardalliance.org
[W33] Open card Framework Sistema abierto, http://www.openscdp.org
[W34] Gemalto Fabricante de tarjetas, http://www.gemalto.com
[W35] Algoritmo RSA, http://www.cesg.gov.uk/publications/media/nsecret/notense.pdf
[W36] Algoritmo RSA, ftp://ftp.rsasecurity.com/pub/pkcs/ascii/examples.asc
[W37] Algoritmo RSA, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html
[W38] Productos de tarjeta Mifare, www.tarjetasmifare.com.ar
[W39] Tarjetas Felica, htp://www.sony.net
[W40] Framework Smart cards Australia, http://www.finance.gov.au
[W41] Data card, http://www.datacard.com
[W42] Institute Enterprise Architecture Developments, http://www.enterprise-architecture.info/
[W43] Instituto Administración de proyectos PMI, http://www.pmi.org

Acrónimos

ADM	Architecture Deveploment Method (Método de desarrollo de arquitectura)
AES	Advanced Encryption Standard (Estándard avanzado de cifrado)
ANSI	American National Standards Institute (Instituto Nacional Americano de Estándares)
APDU	Application Protocol Data Unit (Unidades de datos para aplicaciones de protocolo)
API	Application Programming Interfaz (Interfaz de programas de aplicación)
CC	Common Criteria (Criterios comunes)
CIN	Card Identification Number (Número de Identificación de la Tarjeta)
CISC	Complex Instructions Set Computing (Conjunto de instrucciones de computación complejas)
CMOS	Complementary Metal Oxide Semiconductor (Semiconductor complementario de metal oxido)
COBIT	Control Objetives for Information and related Technology (Objetivos de control para tecnología de información y relacionada)
CRN	Card Reference Number (Número de Referencia de la Tarjeta)
DES	Data Encryption Standard (Estandárd cifrado de datos)
DF	Dedicate File (Archivo Dedicado)
EAL	Evaluation Assurance Level (Nivel de Evaluación del Aseguramiento)
EC	Enterprise Continum (Continuidad de la empresa)
EEPROM	Erase Electrical Programmable Read Only Memory (Memoria sólo lectura borrable programable eléctricamente)
EF	Elementary File (Archivo Elemental)
EMV	Europay Master Visa
EPROM	Erase Programmable Read Only Memory (Memoria sólo lectura borrable programable)
FEA	Federal Enterprise Architecture (Arquitectura Empresarial Federal)
FIPS	Federal Information Processing Standards (Estandáres Federales de Procesamiento de la Información)
GP	Global Platform
GPD	Global Platform Devices (Dispositivos Global Platform)
GSM	Global System for Mobile Communications (Sistema global de comunicaciones móviles)
HSM	Hardware Secure Module (Módulo de hardware seguro)
ICAO	International Civil Aviation Organization (Organización Internacional de Aviación Civil)
IEC	International Electrotechnical Commite (Comité Internacional Electrotécnico)
IEEE	Institute of Electrical and Electronics Enginners (Instituto de

	Ingenieros Eléctricos y Electrónicos)
ISO	International Standards Organization (Organización Internacional de Estandarización)
ITIL	Information Technology Infraestructure Library (Biblioteca de infraestructura de tecnología de la información)
ITSFM	Information Technology Security Evaluation Criteria (Criterios de Evaluación de Seguridad de Tecnología de la Información)
ITU	International Telecommunications Union (Union Internacional de Telecomunicaciones)
JCRE	Java Card Runtime Execution (Ambiente de ejecución de Java Card)
JCVM	Java Card Virtual Machine (Máquina virtual de Java Card)
JVM	Java Virtual Machine (Máquina Virtual de Java)
KMS	Key Management System (Sistema administrador de llaves)
MAC	Messages Authentication Code (Códigos de mensajes de autenticación)
MF	Master File (Archivo maestro)
NITS	National Institute of Standards Technology (Instituto Nacional de Estandáres de Tecnología)
OECD	Organization for Economic Co-Operation and Deveploment
OPEN	Open Platform Environment (Ambiente Global Platform)
PC/SC	Personal Computer/ Smart Card
PIN	Personal Identification Number (Número de Identificación Personal)
PKCS	Public Key Criptography Standard (Estándard de Cifrado de Llave Pública)
PROM	Programmable Read Only Memory (Memoria programable sólo lectura)
PSO	Performance Security Operation (Ejecución Operacion con Seguridad)
ROM	Read Only Memory (Memoria sólo lectura)
RSA	Rivest, Shamir, Adleman (Algoritmo de cifrado asimétrico)
SEI	Software Engennering Institute (Instituto de Ingenieria del Software)
SIB	Standard Information Base (Estandáres de Información Base)
SIM	Subcriber Identity Module (Modulo Identificador del Subscriptor)
STIP	Small Terminals Interoperability Platform (Plataforma de Interoperabilidad de Pequeñas Terminales)
TLV	Type Length Value (Tipo Longuitud Valor)
TOGAF	The Open Group Architecture Framework
TQdM	Total Quality data Management (Administración Total de la Calidad de Datos)
UART	Universal Asynchronous Receiver Transmitter (Receptor Transmisor Asincrono Universal)

Anexos

Anexo 1 Matriz de comandos APDU-Ciclo de vida de tarjetas

Anexo 2 Matriz RACI

Anexo 3 Cronograma del plan de migración e implementación del SGTI