PLATAFORMA PARA SERVICIOS DE FACTURACION Y PAGO EN AMBIENTES MOVILES UBICUOS

Tesis de Maestría
Zeida María Solarte Astaíza

Director: Mag. Oscar Mauricio Caicedo Rendón

Universidad del Cauca
Instituto de Postgrados en Electrónica y Telecomunicaciones
Maestría en Ingeniería, Área Ingeniería Telemática
Departamento de Telemática
Línea de Investigación en Servicios Avanzados de Telecomunicaciones
Popayán, Diciembre de 2008

Dedico este trabajo a mis padres, a mi mamá por su infinita confianza y a mi papá porque aunque no alcanzó a presenciar el final de este proceso, desde el cielo se lo orgulloso que está de mi. A mis tres hijos, Alejandro, Mauricio e Isabella, porque su presencia ha sido y será siempre el motivo más grande que me impulsa en la consecución de mis metas y a mi esposo Julio César por su colaboración, comprensión, tolerancia y gran apoyo que unidos a su gran amor facilitaron mi camino durante el transcurso de la maestría.

Agradecimientos

Quiero expresar mis más sinceros agradecimientos:

Al Dr. Álvaro Rendón, por permitirme el ingreso a la maestría y darme la oportunidad de alcanzar un peldaño más en mi formación profesional.

A mi director de tesis Oscar Mauricio, por su predisposición permanente para aclarar mis dudas, su eficaz guía durante todo el proceso y en especial por su amistad.

A mis compañeros de la maestría por su amistad incondicional y por los momentos gratos que pasamos en las aulas de clase.

A mis compañeros y directivos de la Universidad Autónoma de Occidente por facilitarme las condiciones necesarias para poder cumplir con los compromisos adquiridos y por su apoyo constante.

Resumen

La Computación ha pasado por dos etapas: la de las computadoras centralizadas con gran poder de procesamiento y la del Computador Personal. En el horizonte cercano aparece una que ha sido denominada como computación ubicua, la cual, permite que servicios y aplicaciones residentes en dispositivos móviles o fijos se auto-ejecuten de acuerdo al contexto del usuario, y que dichos dispositivos tengan la capacidad y la inteligencia de regular el procesamiento y el intercambio de información de acuerdo a las necesidades circunstanciales del mismo. Esto hace que las tecnologías ubicuas y los servicios que sobre ellas se implementan, presenten nuevos retos relacionados con la gestión de la seguridad (privacidad, autenticación, autorización, no repudio, entre otros.

Por otro lado, los sistemas de pago han evolucionado al mismo tiempo que lo han hecho las tecnologías computacionales, se ha pasado del simple intercambio de monedas al comercio vía telefónica o por el Internet. Esta revolución también ha digitalizado el proceso de pago, la información de las transferencias financieras es posible enviarla sobre redes abiertas, sin contacto físico entre el comprador y el vendedor. El reciente desarrollo de redes de alta velocidad y redes de datos móviles ha creado un nuevo canal para el comercio, unido a los sofisticados dispositivos móviles que están permitiendo el intercambio virtual de información de pago.

Asociar estas dos tendencias, la computación ubicua y la evolución de los sistemas de pago, es un reto que permite potenciar ambos aspectos, ya que los servicios de pago exigen además de las características propias de los ambientes ubicuos centrarse en características específicas como la seguridad y la privacidad.

En Colombia y gran parte del mundo los servicios ubicuos están emergiendo con gran fuerza. Por tanto, se considera de gran importancia empezar su estudio, concepción, desarrollo, implementación e implantación en nuestro País, para tratar de evitar el rezago tecnológico que tantas otras veces hemos sufrido. Para lograr una primera aproximación colombiana a este tipo de servicios, en este proyecto se presenta una plataforma de facturación y pago de servicios en ambientes móviles ubicuos que permitirá principalmente el estudio y apropiación de los principales aspectos tecnológicos y de seguridad asociados a los sistemas de pago presentes en este tipo de computación y su contextualización en el entorno Colombiano.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Capítulo 1
SISTEMAS DE PAGO EN AMBIENTES UBICUOS

1.1. Ambientes Ubicuos

El termino Computación Ubicua fue introducido por Mark Weiser en 1991. Según Weiser la computación ubicua se describe como computadores muy pequeños con capacidad de comunicación y de computación que se incrustan de forma casi invisible en cualquier tipo de dispositivo cotidiano. Estos dispositivos se encuentran por todas partes y se integran de forma amigable con los humanos, siendo casi imperceptibles para ellos [1].

Por esto, la computación ubicua permite a servicios y aplicaciones que residen en dispositivos móviles o fijos ejecutarse de acuerdo al contexto del usuario sin necesidad de ser activados, y además que dichos dispositivos tengan la capacidad y la inteligencia de regular el procesamiento y el intercambio de información de acuerdo a las necesidades circunstanciales del mismo [2].

La visión de Weiser día a día se está convirtiendo en una realidad, lo cual se puede ver reflejado en parte, en la gran variedad de dispositivos que las personas llevan consigo en cualquier momento, celulares, PDA (*Personal Digital Asistent*- Asistente Digital Personal), computadores portátiles, entre otros, que les permiten acceder a diferentes tipos de aplicaciones y servicios sin importar el lugar, la hora y el dispositivo. Todo esto se hace una realidad, en parte, gracias a las redes inalámbricas que también han evolucionado ampliamente permitiendo que los dispositivos con capacidades de comunicación formen redes de manera espontánea sin requerir infraestructura. Además, al ser móviles los dispositivos personales, estas redes permiten topologías cambiantes, ya que los dispositivos pueden entrar y salir de la red en cualquier momento [3].

A pesar de lo anterior, existen aún algunos aspectos que deben ser desarrollados y los cuales representan retos de investigación para que la computación ubicua y sus servicios sean ampliamente desplegados y aceptados por los usuarios [4].

Uno de estos aspectos es el modelo económico asociado al cobro de los servicios ubicuos el cual debe garantizar el retorno a la inversión de manera efectiva ya que este tipo de servicios no son subsidiados, como lo fue el servicio de internet en sus comienzos, ni son ofrecidos de manera única por grandes operadores como lo es la telefonía móvil, en este tipo de servicios, dadas sus características, entran en juego muchos más empresas de diferentes tipo y personas de manera individual. Basados en la experiencia de los servicios por Internet, en [5] se describen algunos modelos que inicialmente podrían generar un retorno a la inversión para los servicios ubicuos ofrecidos.

- Servicios Subsidiados. En este modelo el costo por el ofrecimiento del servicio ubicuo es cubierto a través de los ingresos que se generan por el uso de otros servicios. Respecto a los ambientes ubicuos presenta el inconveniente de necesitar un complejo esquema contractual

entre todas las partes que intervienen en el negocio, por otro lado, en determinadas circunstancias los servicios a través de los cuales se están subsidiando los servicios ubicuos se volverían demasiado costosos, y por ultimo dada las características de los servicios ubicuos ellos deberían poder ser ofrecidos en cualquier sitio y no siempre existe la posibilidad de que en el entorno hayan empresas que los subsidien.

- Basado en ingresos por publicidad. Este modelo ha sido ampliamente usado en Internet, así, los servicios no son pagados por los usuarios sino por las empresas o negocios que ponen la publicidad, de esta manera se espera que este modelo también sea aplicado a los servicios ubicuos, sin embargo en estos ambientes se debe tener un balance entre la privacidad de los usuarios y los intereses de las empresas que publicitan. Por ejemplo: si el usuario del servicio escoge bloquear la publicidad esto generará menores ingresos para el proveedor del servicio [6].
- Pago por uso del servicio. En este modelo los ingresos por el uso de los servicios son pagados directamente por los usuarios, ejemplo, el servicio de telefonía móvil. Proporciona una gran flexibilidad, alcance y facilita la generación de ingresos, es el modelo más usado para el cobro de diferentes clases de servicios y por lo tanto sería aplicable a los servicios ubicuos. Requiere de una infraestructura de pago eficiente y confiable que genere satisfacción y confianza en los usuarios.

1.2. Sistemas de Pago Electrónico

Los sistemas de pago están asociados a la necesidad de intercambiar valor, son tan antiguos como la misma civilización y han evolucionado al ritmo de ella. En el siglo XVII aparece el dinero en papel el cual era respaldado por reservas de oro. La evolución continuó durante el siglo XX hasta el sistema actual en el que el papel moneda y los depósitos en cuentas de banco se consideran dinero porque tienen el respaldo de los gobiernos. En este contexto histórico, el "dinero en plástico" y el "dinero electrónico" son innovaciones muy recientes [7].

Las tarjetas de crédito emitidas por bancos y comercios minoristas se utilizan en todo el mundo desde los años 1950. Durante la década siguiente, las organizaciones mundiales de tarjetas de crédito tales como Visa y MasterCard lograron una mayor aceptación entre los comerciantes consolidando marcas. Esto sentó las bases para los primeros sistemas de pago electrónico a principios de la década de 1970, durante la cual se introdujeron tarjetas de crédito con banda magnética y la aprobación automática de transacciones con ellas. Los primeros cajeros automáticos y tarjetas de débito surgieron en los años 1980, completando la integración del papel y el dinero en plástico. Las tarjetas de crédito y de débito siguen siendo el método de pago no tradicional (efectivo) más utilizado para las transacciones minoristas, pero durante los últimos años han aparecido nuevas tecnologías tales como los débitos directos y los créditos basados en Internet [7].

La introducción de nuevas tecnologías ha transformado la industria de pago y el comportamiento de los consumidores con respecto a la forma de hacer los pagos. Antes del auge de la Internet los consumidores podían comprar en los almacenes o a través de catálogos vía correo físico o por teléfono. Actualmente un gran porcentaje de las personas hacen compras en línea. En los almacenes, el efectivo y los cheques están siendo ampliamente reemplazados por métodos de pago electrónico, en especial por las tarjetas débito y crédito [8]. El creciente uso de estos sistemas de pago ha generado numerosos beneficios, incluyendo la conveniencia y la reducción de

costos para compradores y vendedores, así como un crecimiento acelerado de la economía, un nivel superior de seguridad y una mayor movilidad internacional.

Entre los productos de pago electrónico más relevantes se encuentran:

Productos de pago basados en tarjetas.

- Tarjetas de pago convencionales: una tarjeta de crédito es un plástico con una banda magnética y un número en relieve que sirve para hacer compras y pagarlas en fechas posteriores. Las marcas de mayor renombre son Visa, MasterCard, American Express, y Diners Club. Las tarjetas que exigen el pago total del saldo cada mes se conocen como "*charge cards*" (tarjetas de crédito sin financiamiento), mientras que las tarjetas de crédito otorgan crédito renovable.
- Tarjetas débito: con la llegada de los cajeros automáticos, los bancos comenzaron a emitir "tarjetas de clientes" para que éstos pudieran tener acceso a sus cuentas. En muchos países posteriormente establecieron redes para permitir la interoperabilidad. Las tarjetas de débito no sólo se pueden utilizar en cajeros automáticos sino que ofrecen un método directo de pago a comerciantes equipados con las terminales correspondientes.
- Tarjetas inteligentes: el desarrollo de la tecnología de tarjetas inteligentes a mediados de 1980 permitió la adición de nuevas aplicaciones para tarjetas de pago, utilizando un microprocesador o chip de memoria integrado a las mismas. Además de la funcionalidad tradicional de débito y crédito, las aplicaciones incluyen la capacidad de realizar transacciones por Internet usando un lector de tarjeta inteligente adjunto a una computadora personal. Los más avanzados de estos sistemas son multi-aplicaciones basadas en Java que también pueden descargar aplicaciones individualizadas. Las ventajas de estas tarjetas sobre las tradicionales (con banda magnética) son la inclusión de mecanismos de codificación/decodificación de alta seguridad y la capacidad de almacenar datos dinámicos tales como los detalles de compra, útiles para sistemas avanzados de lealtad de los clientes [7].
- Tarjetas inteligentes sin contacto: incluyen un micro-controlador seguro, memoria, y una interface que lo conecta a un dispositivo lector, esta interface normalmente es una pequeña antena embebida en la tarjeta. El dispositivo se conecta con el lector a través de radiofrecuencia, sin requerir contacto físico [9].

Pagos por Internet

El rápido aumento en la penetración de Internet durante los últimos años ha dado lugar a una gran variedad de nuevos sistemas de pago electrónico. Las tarjetas de pago emitidas por bancos que utilizan sus sistemas de autorización/compensación/liquidación existentes han cimentado el camino para nuevos sistemas que permiten los créditos y débitos directos entre cuentas bancarias en muchos mercados. Cuando se introdujeron inicialmente, los débitos directos funcionaban solamente al interior de bancos individuales y esto limitaba su uso a los proveedores tales como compañías de servicios públicos que eran lo suficientemente grandes para tener cuentas en todos los bancos utilizados por sus clientes. Por el mismo motivo, los créditos directos se usaban principalmente para las recaudaciones regulares como depósitos de nómina. Gracias a las nuevas redes electrónicas interbancarias en muchos mercados ahora se pueden realizar débitos y créditos directos iniciados por el cliente "*ad hoc*" que son virtualmente instantáneos o toman de dos a tres días. No obstante, los productos de pago basados en tarjetas continúan dominando este segmento en cuanto a participación de mercado [7].

Pagos móviles

El MPF (*Mobile Payment Forum* - Foro de Pagos Móviles) define un pago móvil como el proceso en el cual dos partes intercambian valores financieros usando un dispositivo móvil en retorno de artículos o servicios. En este contexto, se consideran dispositivos móviles a los dispositivos que permiten comunicación inalámbrica tales como teléfonos celulares, teléfonos inteligentes, PDA, computadores portátiles entre otros [10].

La información del pago es transportada por un operador de red móvil y usa un protocolo basado en Web, como WAP (*Wireless Access Protocol*- Protocolo de Acceso Inalámbrico) o HTML (*HiperText Markup Language* – Lenguaje de Marcado de Hipertexto), o un sistema de mensajería como SMS (*Short Message Service* – Servicio de Mensajería Corta). Alternativamente el transporte de dicha información podría hacerse, en el caso de los pago por proximidad, vía Bluetooth, Infrarrojos, RFID (*Radio Frequency IDentification* - Identificación por Radiofrecuencia), NFC (*Near Field Communication* - Comunicación por Campo Cercano).

Los pagos móviles pueden clasificarse teniendo en cuenta diferentes aspectos de las transacciones involucradas [11]. Entre todas estas clasificaciones hay dos basadas en características bastante relevantes para la definición de una arquitectura para un sistema de pago dentro de un ambiente ubicuo, la ubicación del usuario en el momento de realizar el pago, y el monto a pagar, el cual determina en gran parte que tan fuertes deben ser los mecanismos de seguridad.

Según la ubicación del usuario se pueden presentar dos opciones: Pagos remotos y pagos por proximidad [12].

- El pago remoto se refiere al pago que se efectúa a través de un dispositivo móvil, sin necesidad de la presencia física del usuario en el punto de venta. La tecnología más comúnmente usada en este caso es SMS.
- El pago por proximidad exige que el usuario con su dispositivo móvil se encuentre en el punto de venta para ejecutar el pago. Podría ser usado directamente en una tienda, en un punto de venta desatendido, en una máquina expendedora de tiquetes o en un kiosco. En este método los consumidores apuntan o pasan su móvil por un lector específico, para enviar los datos al sistema de pago, para lo cual emplean alguna tecnología inalámbrica como Bluetooth, infrarrojo, RFID o NFC.

Según el monto del pago los pagos móviles pueden ser micro o macro pagos:

- Micro pago: son pagos móviles donde el monto es una pequeña cantidad de dinero, brindando la capacidad de un procesamiento rápido y de generar sobrecostos muy bajos [13]. Algunos autores definen un valor de alrededor de los 10 dólares para delimitar estos pagos [14]
- Macro pago: contrario a la definición anterior, los macro pago son aquellos sistemas que manejan transacciones de un valor relativamente alto. Ejemplos típicos de los sistemas de macro pago incluyen las tarjetas de crédito, las suscripciones, y los cheques de banco. El valor de las transacciones del macro pago es generalmente alto, tales sistemas son caracterizados por requerir fuertes medidas de seguridad, ya que por ejemplo, el hurto del número de la tarjeta de crédito o un número de cuenta bancaria podría resultar en la pérdida de una

cantidad significativa de dinero de los usuarios o comerciantes. Como resultado de este deseo de una seguridad y los requisitos de facturación, los sistemas de macro pago incurren típicamente en altos costos de operación en términos computacionales, costos de instalación, y honorarios de proceso [5].

1.3. Sistemas de Pagos Móviles por Proximidad

Los pagos por proximidad permiten que el proceso de pago sea más natural ya que se realizan en el punto de venta y en tiempo real, además no implican procedimientos complejos ni demoras en las transacciones, lo que los hace adecuados para ser implementados en ambientes ubicuos.

Como se explicó en el numeral anterior un pago por proximidad es aquel en donde el consumidor está físicamente presente en el punto de venta en el momento de su realización. Asociado a este tipo de pago debe existir una interfaz de proximidad la cual tiene como función transferir las credenciales de la transacción entre el dispositivo móvil y el terminal en el punto de venta. La interfaz de proximidad puede ser implementada usando una gran variedad de tecnologías de no contacto, entre las cuales se encuentran la identificación por radiofrecuencia (RFID) [15], y los estándares de conectividad de corto alcance (NFC) [16], entre otras.

En el caso de los pagos por proximidad tanto la aplicación de pago como la información de la cuenta se cifran y cargan en un área segura del dispositivo móvil, la cual se implementa con una etiqueta de tecnología RFID o NFC incrustada, a través de este elemento seguro se establece una comunicación con el lector ubicado en el punto de venta del almacén.

Los pagos móviles por proximidad pueden ser realizados tanto en puntos de venta atendidos (almacén) como en desatendidos (máquina expendedora). Para realizar el pago, el consumidor simplemente acerca el dispositivo móvil al lector ubicado en el punto de venta y el pago se efectúa.

Los pagos por proximidad están adquiriendo un gran interés tanto por la industria móvil como por la financiera, y a pesar de que las motivaciones que han impulsado este interés son de diversa índole, según el Foro de Pagos Móviles, la principal ha sido la conveniencia de dichos métodos de pago [17]. Las características principales que hacen convenientes a los pagos por proximidad son:

- Velocidad: los pagos por proximidad se efectúan de manera mucho más rápida que los tradicionales.
- Mínima intervención del usuario: las operaciones son simples y muy fáciles de usar.
- Integración: incorporación de servicios con el instrumento de pago y la posibilidad de interactuar con él sin requerirse de un lector separado.

La implementación de pagos móviles por proximidad involucra una gran cantidad de actores [18], como se muestra en la Figura 1.

- Operadores móviles, quienes prestan la infraestructura de comunicaciones para permitir el envío de notificaciones a los usuarios.
- Fabricantes de dispositivos, encargados de habilitar los dispositivos móviles con las tecnologías necesarias para realizar los pagos.

- Desarrolladores de software para pagos, encargados de desarrollar el software necesario para que los pagos se puedan realizar desde los dispositivos móviles.
- Emisores, corresponden a las entidades financieras encargadas del manejo de la cuenta bancaria del usuario.
- Consumidores, se refieren a los usuarios que efectúan los pagos.
- Comerciantes, dueños de los almacenes que comercializan los productos y permiten los pagos por proximidad desde sus puntos de venta.

Figura 1. Actores involucrados en un sistema de pago por proximidad
Fuente: A Smart Card Alliance Contactless Payments Council White Paper. 2007

1.4. Características de los Sistemas de Pago en Ambientes Ubicuos

Un sistema de pago en un ambiente ubicuo combina dos situaciones que deben ser tenidas en cuenta a la hora de definir sus características, las particularidades propias de los ambientes ubicuos y las características de los sistemas de pago, las cuales deben ser combinadas para obtener un sistema adecuado.

Miembros de la comunidad científica están de acuerdo en que la computación ubicua debe tener como base los siguientes elementos [19]:

- En la computación ubicua se manejan dispositivos de cómputo no tradicionales, tales como dispositivos muy pequeños o casi invisibles, los cuales están inmersos en el ambiente físico.
- Las aplicaciones ubicuas generalmente involucran un gran número de estos dispositivos no tradicionales.
- Los nuevos dispositivos de cómputo están usualmente equipados con sensores que permiten captar información del entorno.

- La mayoría de los nuevos dispositivos son móviles y las tareas para las cuales están programados se ejecutan de acuerdo a su posición geográfica y la de otros dispositivos en su vecindario. Ya que muchos de los dispositivos no están fijos en el sistema, la computación ubicua debe permitir formar redes espontaneas.
- Dada la característica intrínseca de la computación ubicua de introducirse dentro de la vida cotidiana de las personas [20], la implementación de servicios en estos ambientes deberán manejar de manera muy cuidadosa aspectos relacionados con la privacidad y la seguridad.

Por otro lado, se tienen las características que deben tener los sistemas de pago electrónicos [21], entre las cuales es importante destacar las siguientes: rápidos, de bajo costo y garantizar la privacidad y la seguridad de la información a transferir a través de medios electrónicos.

Todo lo anterior permite determinar las principales características de los sistemas de pago en ambientes ubicuos, las cuales se describen a continuación [5].

1.4.1. Espontaneidad

Un ambiente ubicuo puede contener componentes de infraestructura, los cuales son más o menos fijos, y componentes basados en dispositivos que entran y salen periódicamente del entorno. En un sistema ubicuo, normalmente con un ambiente dinámico, estos componentes deben poder interoperar de manera espontánea. Un componente interopera espontáneamente si es capaz de interactuar con un conjunto de componentes de comunicación que pueden cambiar de identidad y de funcionalidad cuando las circunstancias se modifican. Los componentes de interacción espontáneos cambian durante su operación normal cuando se mueven o cuando otro componente entra a su ambiente.

Por lo anterior, los mecanismos de pago para servicios ubicuos no deben requerir que los individuos establezcan unas relaciones demasiado complejas con los proveedores de servicio involucrados en el pago. Los sistemas de pago deberían permitir a los usuarios adoptar modelos "*pay as you go*" (páguelo cuando lo use) para el uso de los servicios [5].

1.4.2. Eficiencia

En situaciones en donde el usuario y el proveedor del servicio no tienen establecida una relación de confianza se requieren sistemas de pago muy eficientes ya que generalmente en este tipo de relaciones los pagos son de montos muy bajos, por lo tanto, es importante que el sistema de pago sea liviano y eficiente, caracterizado por costos de comunicación y computación bajos, acoplados con recargas financieras mínimas [13].

Las consideraciones relacionadas con las comunicaciones y la computación son especialmente importantes en los ambientes ubicuos por las limitaciones de recursos que típicamente vienen asociadas con los dispositivos utilizados. Por otro lado, muchos esquemas de pago existentes incurren en sobrecostos financieros altos por cada transacción (por ejemplo las tarjetas de crédito), lo cual es inaceptable en ambientes ubicuos donde se manejen transacciones de bajo valor.

1.4.3. Seguridad

La seguridad es uno de los aspectos más importantes en el campo de los pagos móviles, independiente de su clasificación, ya que sin un intercambio seguro de la información comercial y sin transacciones financieras seguras no es posible desarrollar modelos de pago confiables para los usuarios.

Un sistema de pago seguro debe tener las siguientes características [22]:

- Confidencialidad: la información debe ser asegurada contra personas, procesos o dispositivos no autorizados. Consiste en asegurar que los datos enviados en una comunicación no pueden ser leídos por una persona distinta al destinatario final, o que si ocurre esto, el espía no pueda entender el mensaje enviado, o en su defecto, que cuando consiga obtener éstos datos ya no le sirvan. Es decir, se debe garantizar que ninguna persona ajena a la transacción pueda tener acceso a los datos de la misma.
- Autenticación: consiste en asegurar que los participantes en la transacción no son impostores. Las entidades participantes en una transacción comercial electrónica deben estar perfecta y debidamente identificadas antes de su inicio. Es decir, los participantes de la comunicación deben estar seguros que la persona con la cual van a establecer una comunicación es realmente quién dice ser, de lo contrario, se puede facilitar datos íntimos y/o sensibles a una persona o entidad no deseada, quien podría hacer uso malintencionado de los mismos.
- Integridad: garantiza que la información y los sistemas no han sido alterados ni corruptos por agentes externos. Es necesario estar seguro que los datos enviados en una comunicación llegan íntegros, sin modificaciones, a su destino final. Esto es, que la información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y borre.
- Autorización: verifica que el usuario tiene los permisos para hacer las transacciones requeridas. La autorización está muy relacionada con la autenticación, cuando un participante se autentica antes de dar inicio a la transacción, se debe determinar a qué información puede acceder y qué tareas está en capacidad de acometer. Este proceso determina los privilegios asociados a un perfil de usuario.
- Disponibilidad: el sistema debe ser accesible en todo momento para los usuarios autorizados. Forma parte de la seguridad el poder disponer de la información cuando se necesite. Por ello se deben proteger los sistemas de forma que se mantengan en funcionamiento y se pueda acceder a la información en cualquier momento.
- No repudio: asegura que el usuario no pueda negar que ha ejecutado una transacción y deberá proveer pruebas si tal situación ocurre. Se debe asegurar que una vez enviado un mensaje con datos importantes o sensibles el destinatario de los mismos no pueda negar haberlo recibido, o si es el caso del emisor éste no pueda negar su transmisión.

La seguridad en los pagos móviles se debe manejar desde muchos frentes:

- Seguridad de los dispositivos móviles: ya que los dispositivos móviles contienen datos confidenciales de los usuarios y son más propensos al robo y a daños, se requiere que se establezcan medidas de protección para ellos. En este sentido, por ejemplo, la seguridad frente a uso no autorizado puede ser establecida mediante mecanismos de autenticación del

usuario y un almacenamiento seguro de los datos y niveles de seguridad en los sistemas operativos. Generalmente en los dispositivos móviles que almacenan información confidencial, esta es guardada en elementos seguros con los niveles más altos de protección. El nivel de seguridad de los dispositivos necesita estar incrementándose de manera continua y esto en gran parte es potestad de los fabricantes de tales dispositivos [22].

- Seguridad en las tecnologías de red: la información confidencial de los usuarios debe ser protegida contra intercepciones cuando ella es enviada a través de las diferentes tecnologías de red inalámbricas. GSM (*Global System for Mobile communications* – Sistemas Global para comunicaciones Móviles) provee mecanismos de seguridad básicos, como la autenticación de los usuarios y enlaces cifrados a través de claves simétricas, pero aún así existen problemas de seguridad ya que no existen mecanismos de autenticación en las estaciones móviles, en este sentido el esquema de seguridad que implementa UMTS (*Universal Mobile Telecommunications System* – Sistema Universal de Telecomunicaciones Móviles) es mucho más completo. Por otro lado las redes WLAN (*Wireless Local Area Network* – Red Inalámbrica de Área Local) y WPAN (*Wireless Personal Area Network* – Red Inalámbrica de Área Personal) que trabajan en las bandas de frecuencia no licenciadas aún presentan problemas de seguridad bastante grandes, el esquema básico que este tipo de redes maneja cifrado de datos por medio de claves [22].
- Seguridad a nivel del servicio: Si la seguridad a nivel de dispositivo y a nivel de red no es suficiente, se requiere implementar mecanismos de seguridad en las aplicaciones de pago, los cuales pueden involucrar la autenticación de los usuarios a través de claves secretas, la certificación por parte de entidades ampliamente confiables de los participantes en la transacción, el cifrado de los datos, entre otros.

1.4.4. Privacidad

La privacidad es un aspecto de gran importancia asociada a la computación ubicua y por ende a los servicios asociados, entre ellos los de pago. Muchas de las comunidades de investigadores reconocen el riesgo inherente que representa un sistema invisible, intuitivo e intrusivo para las normas sociales actuales y los valores relacionados con la privacidad y la vigilancia de los individuos [23].

Estos riesgos de privacidad propios de la computación ubicua y sus servicios se deriva de dos innovaciones tecnológicas actuales que son necesarias para su éxito [23]: el aumento de la capacidad para recopilar datos de las interacciones cotidianas de las personas (en varias modalidades y por espacios grandes de tiempo y lugar), y una mayor habilidad en la búsqueda rápida en grandes bases de datos, aumentando la posibilidad de crear perfiles de usuarios y otras formas de minería de datos.

Se han identificado un conjunto de aspectos relacionados con la privacidad de las redes ubicuas y sus servicios, que afectarán a los usuarios de los mismos:

- La existencia de una red ubicua de dispositivos traerá como consecuencia que la cantidad de información personal que circula crecerá en gran medida.
- La introducción de interfaces biométricas y perceptuales de ciertas aplicaciones, transformará la naturaleza cualitativa de la información personal en circulación.

- Para poder tener servicios personalizados, propios de estos ambientes, se requerirá la recopilación y el seguimiento de gran información relacionada con la vida diaria de las personas.

1.4.5. Flexibilidad

Se asume que los sistemas ubicuos son altamente volátiles y por tanto no deben asumir configuraciones específicas de red, de usuarios ni de dispositivos. En este sentido, se deben tener en cuenta dos situaciones especiales, la operación sin conexión y la no disponibilidad de los dispositivos.

La operación sin conexión es un modo de funcionamiento en el cual se permite que el cliente siga accediendo al servicio durante fallas temporales, ya sea de los repositorios de los datos o de las conexiones a la red. En un ambiente ubicuo el usuario puede transitar entre redes, lo cual causará desconexiones temporales y por tanto los sistemas de pago no deben diseñarse asumiendo conexiones permanentes.

Por otro lado relacionado con la no disponibilidad de los dispositivos, la interacción de los usuarios con los ambientes ubicuos puede o no involucrar algún dispositivo personal, como una PDA o un teléfono inteligente, así que el sistema de pago debería en lo posible no relacionarse directamente con el dispositivo móvil [5].

1.4.6. Mínima intervención del usuario

Se refiere a la cantidad de acciones que debe llevar a cabo el usuario en el momento de hacer uso del sistema de pago ubicuo, es un aspecto crucial si se tienen en cuenta el gran número de transacciones que una persona podría realizar durante el curso de un día normal. Por ejemplo, los usuarios esperarán un nivel de servicio comparable al existente con las tarjetas de crédito y las cuentas bancarias. La mayoría de los usuarios no aceptaría un sistema que permita que se lleven a cabo transacciones financieras sin su intervención; al mismo tiempo, no es práctica la participación del cliente en todas las transacciones especialmente cuando estas son de bajo valor. Por lo tanto, los diseñadores de los sistemas de pago enfrentan el reto de balancear estas necesidades contradictorias [5].

1.4.7. Despliegue

La capacidad de despliegue es un requisito no funcional que se ocupa de la fiabilidad y facilidad con que las aplicaciones se pueden poner en funcionamiento en el entorno de producción. En el lado del cliente, la capacidad de despliegue tiene que ver con la instalación y actualización de los mecanismos que pueden ser incorporados en el software en sí, lo cual en los ambientes ubicuos debe ser totalmente transparente para el usuario. En el lado del servidor, la capacidad de despliegue se determina por la arquitectura del sistema y su implementación, los cuales deben permitir que el servicio sea desplegado a gran escala y que pueda soportar los antiguos y los nuevos servicios [5].

1.5. Algunas técnicas para garantizar la seguridad

1.5.1. Criptografía

La criptografía se define como el arte de cifrar la información, de tal forma que solo pueda ser descifrada por el receptor a quien está dirigida. Cifrar un mensaje consiste en convertir caracteres en texto plano a una serie de caracteres no legibles, y el descifrado involucra el proceso inverso. La seguridad radica en que solo el receptor sea quien pueda descifrar el mensaje cifrado, para lo cual se emplean algoritmos matemáticos y una llave, que consiste en un número generado aleatoriamente que poseen tanto el emisor como el receptor, que se debe mantener en secreto. Aunque inicialmente los métodos de cifrado contenían una lógica muy sencilla, como intercambiar letras o sílabas, en la actualidad se emplean algoritmos matemáticos complejos y se clasifican en métodos de cifrado simétricos o de llave privada y métodos de cifrado asimétricos o de llave pública [24].

El cifrado simétrico consiste en utilizar la misma llave, tanto para el proceso de cifrado del mensaje en el emisor, como para el de descifrado en el receptor, por lo cual la llave también se transmite al destinatario del mensaje. La llave por razones de seguridad se debe mantener en secreto entre las dos partes que se comunican, por lo cual se convierte en un sistema vulnerable al soportar toda su eficiencia en la confidencialidad de la clave [25]. La gran ventaja de estos sistemas es su sencillez por lo cual los procesadores los manejan fácilmente, siendo así más eficientes y rápidos que los métodos de cifrado asimétricos. Los métodos simétricos más comunes son DES (*Data Encription Standard* – Estándar de Cifrado de Datos), DESX, Triple-DES, RC2 (*Rivest Cipher* – Cifrado de Rivest), RC4, RC5 y AES (*Advanced Encription Standard* – Estándar de cifrado Avanzado) [24].

En el cifrado asimétrico cada participante en la comunicación maneja dos llaves complementarias, una privada y otra pública, con la primera se cifran los mensajes y con la otra se descifran. Es decir un usuario A tiene una llave privada K y una llave pública L, la primera solo la conoce él y la segunda es visible a los demás usuarios, así si otro usuario B desea enviarle un mensaje cifrado asimétricamente, debe cifrar la información con la llave L y A será el único que pueda descifrar el mensaje empleando su llave privada K [26][24]. La ventaja de este tipo de cifrado es que evita que las llaves para descifrar los mensajes se tengan que compartir. La principal desventaja del cifrado asimétrico es su velocidad de ejecución, al ser considerablemente más lento que un esquema de llave simétrica. Los métodos asimétricos más conocidos son: Diffie-Hellman, RSA (*Rivest Shamir Adleman Algorithm* – Algoritmo de Rivest Shamir Adleman) y DSS (*Digital Signature Standard* – Estándar de Firma Digital)[24].

El cifrado asimétrico trae consigo problemas de velocidad de procesamiento y el simétrico por el tamaño de sus llaves, en algunos casos no resulta confiable para los usuarios. Por lo cual se han creado sistemas donde se combinan, tratando de aumentar la eficiencia sin que esto resulte en procesos demasiado lentos [27].

La combinación consiste en emplear una llave privada para cifrar y para descifrar el mensaje, es decir un esquema simétrico, pero para el envío de la llave se emplea un esquema asimétrico. Es decir, un usuario A utiliza una llave privada Ks (llave de sesión) para cifrar el mensaje, el cual es enviado a un usuario B. Además cifra la llave Ks con la llave pública de B, el cual para poder leer el

mensaje debe primero descifrar la llave Ks con su llave privada, y finalmente utiliza Ks para descifrar el mensaje [24].

1.5.2. Proceso de Certificación

La certificación es un sistema de seguridad para generar confianza en el intercambio de información vía telemática, otorga a las distintas partes, que intervienen en un proceso, la seguridad necesaria para interactuar en un entorno en el que nadie se conoce. Este proceso incluye varios conceptos como las autoridades de certificación, las firmas digitales y los certificados digitales.

Una Autoridad Certificadora (CA – *Certication Authority*) es una entidad, que puede ser una empresa, una entidad gubernamental u otro usuario de la red, que tiene como función principal avalar si una llave pública pertenece al usuario que la posee. Para lograr su propósito, la CA emplea certificados digitales, que es el medio formal para garantizar la autenticidad de una llave pública al llevar una firma digital de la entidad que lo expidió, por lo cual es importante que esta CA sea de confianza para cada uno de los usuarios. Para generar esta confianza se establecen relaciones entre las CA y los usuarios, o entre las CA cuando existen varias, siguiendo modelos ya establecidos como: CA único, jerárquico, igual a igual o en malla [28].

La función principal de una Autoridad Certificadora es administrar los certificados de una red, que incluye varias actividades como generar, firmar, distribuir y revocar certificados, generar una lista CRL (*Certificate Revocation List* – Lista de Revocación de Certificados) con los certificados revocados, autenticar usuarios, y procesar solicitudes de Certificados. Para esta última función las CA se apoyan en otra entidad llamada RA (*Register Authority* - Autoridad de Registro) que se encarga de recoger todos los datos y llave pública del usuario, además de comprobar su autenticidad [27].

La firma digital consiste en un código generado a partir de la clave privada, que se utiliza para proporcionar a una entidad un medio para enlazar su identidad a una pieza de información, además se emplea para propósitos de autenticación, integridad de datos y no repudio. La firma digital autentica el documento cifrado, ya que la información solo puede ser descifrada con su llave pública, con lo cual el receptor verifica la firma [29].

En la actualidad, para una firma digital no se cifran completamente los documentos para ahorrar tiempo, por lo cual se utilizan funciones hash, que son una vía matemática para transformar una cierta cantidad de información de tamaño variable en un bloque de tamaño específico, que es posteriormente cifrado con la llave privada del emisor, obteniendo así la firma digital. Luego esta firma se concatena con el mensaje original y es enviado al destinatario, el cual descifra la información con la llave pública del emisor. El receptor pasa el mensaje original por la misma función hash y si el resultado de esta operación es igual al mensaje descifrado, la firma es válida [29].

La firma digital descrita anteriormente no es suficiente garantía para comprobar la autenticidad de una llave, por lo tanto se requiere de un certificado digital, que es un archivo con información que vincula una llave pública con la identidad de una entidad, con lo cual se puede verificar si la llave pertenece a quien dice poseerla [29].

Los certificados son un medio eficiente para crear confianza en la criptografía de llave pública y en general contiene las siguientes tres piezas de información: el nombre del sujeto para quien se haya expedido el certificado, la llave pública y una firma digital del emisor del Certificado o Autoridad Certificadora. La firma digital se encarga de verificar la información del certificado, y si tiene éxito, el certificado en sí es quien comprueba la pertenencia de la llave pública a un usuario determinado [29].

El formato más común para los certificados es el X.509, que es un estándar de la ITU (Unión Internacional de Telecomunicaciones) y la ISO/IEC (Organización Internacional de Estándares/ Comisión Electrotécnica Internacional) publicado en 1988. Después, se publicó una segunda versión en 1993 y una tercera en 1996, la cual se encuentra vigente actualmente y está definida por el RFC 3280. Se han definido varios campos en la versión 3 de X.509 [28]: número de versión (V3 actualmente), número serial del certificado, identificador del algoritmo usado para firmar el certificado, nombre de la Entidad que ha emitido el certificado, período de validez del certificado, llave pública, incluyendo el Identificador del algoritmo de llave pública, nombre del sujeto o dueño de la llave pública del ítem anterior, identificador único del emisor y del sujeto, extensiones opcionales y firma digital

1.6. Antecedentes

Alrededor de los pagos móviles se han desarrollado una gran variedad de proyectos que tienen diferentes características y se enfocan en atacar diversas necesidades, pero hasta el momento no existe ninguna solución integral. Las soluciones de pago existentes no son lo suficientemente seguras, son muy difíciles y lentas de usar, o están disponibles solo para una pequeña cantidad de productos o servicios o solo para un grupo reducido de clientes. Algunos de estos sistemas o proyectos se describen a continuación.

- **UPTF** (*Universal Pervasive Transaction Framework*) [30]: consiste en el desarrollo de una plataforma para trabajar en ambientes invasivos que permite la realización de acuerdos entre las diferentes partes participantes de una transacción realizada a través de dispositivos móviles en ambientes inalámbricos inseguros. Se implementaron dentro del proyecto dos sistemas completos para compra y pago a través de dispositivos móviles, en el primero se trabaja con un dispositivo diseñado especialmente para este propósito, mientras el segundo trabaja con teléfonos móviles con soporte a Java ME (*Java Micro Edition*).
- **P2P** (*Paid Peer to Peer M-Payment System*) [31]: propone un sistema de pago móvil de igual a igual que permite a los usuarios móviles llevar a cabo pagos de manera inalámbrica a través de tecnología Bluetooth y además ejecutar las transacciones hacia el servidor de manera segura.
- **PSP** (*Payment Session Protocol*) [32]: brinda soporte a interacciones relacionadas con pagos entre clientes y servidores en ambientes ubicuos. Refleja transacciones comerciales del mundo real y se basa en el intercambio de contratos, los cuales describen las características no funcionales de los servicios, tales como calidad del servicio, costos, términos y condiciones de uso. Permite crear acuerdos a nivel de servicio entre clientes y servidores. PSP está diseñado para funcionar en conjunto con una solución de pago basada en micro pago como Millicent.
- **PayPal** [33]: es un servicio de pago en línea bastante popular, adquirido recientemente por la empresa eBay. A través del uso de teléfonos celulares habilitados con WAP los usuarios pueden usar interfaces inalámbricas de PayPal para realizar los pagos. Con el servicio PayPal Mobile, se puede enviar dinero, comprar artículos, realizar donaciones desde su dispositivo móvil. Los usuarios de este servicio hacen pagos a través del envío de mensajes de texto a

PayPal. PayPal llama al usuario para confirmar el pago móvil, y entonces envía el dinero a la cuenta. En el caso de una compra *Text to Buy*, después de que el comerciante ha recibido el pago, el artículo comprado es enviado a la dirección previamente almacenada en la cuenta PayPal del usuario.

- **MobiPay** [34]: es uno de los sistemas de pago más versátiles, ya que permite macro y micro pagos, se puede usar para hacer transacciones persona a persona (P2P) o para pagar en el punto de venta (POS), e incluso le da al usuario la opción de escoger entre cargar el servicio a la factura telefónica o usar una tarjeta bancaria (débito o crédito).
- **SEMOPS** (*Secure Mobile Payment Service*) [35]: es un sistema de pago amigable al usuario, universal y complejo. Las posibles transacciones que se pueden realizar con este sistema de pago incluyen pagos en puntos de venta, pagos en línea por Internet o WAP, transferencias P2P, compras en máquinas expendedoras y también pagos de facturas. Pueden ser micro o macro pagos. Para los usuarios y los comerciantes, el servicio de pago es provisto por su propio banco o por el operador móvil. Como no existen intermediarios involucrados en el proceso la transacción completa de pago se basa en relaciones de confianza entre las partes. En este sistema, los usuarios no necesitan dar ninguna información sensitiva durante el proceso de pago, por lo tanto ellos pueden aparecer anónimos durante este. Habiendo recibido la información necesaria de la transacción, el usuario prepara y firma un requerimiento de compra y la envía hacia su propio procesador de pago. Si los fondos son suficientes, el comerciante recibe una notificación de pago desde su propio procesador de pago.

De otro lado, en relación a los pagos por proximidad en los últimos años se han desarrollado de manera satisfactoria algunos programas a través del mundo. Entre ellos cabe destacar [18]:

- En junio de 2007, Visa y Wells Fargo anunciaron el lanzamiento de un amplio piloto para probar el consumo de pagos y servicios móviles usando dispositivos móviles equipados con tecnología NFC, el piloto prueba la seguridad, la entrega OTA (*Over The Air* – A través del aire) de la cuenta de pago al dispositivo móvil, pagos móviles en almacenes y restaurantes que acepten tecnología Visa PayWave, recepción y cambio de cupones móviles, y servicios de gestión de cuentas.
- En Junio de 2007, Cellular South anunció el lanzamiento de la primera prueba de consumo de su servicio Wireless Wallet basado en los teléfonos NFC Biométricos de Kyocera y el software Wallet de ViVOtech. Este servicio permitía a los consumidores acceder a su billetera móvil en teléfonos NFC usando su huella digital.
- En abril de 2007, MasterCard inició una prueba de pago móvil con teléfonos NFC y que tuvieran capacidades PayPass. Esta prueba se realizó en Hong Kong e integró a Hong Kong Retail Technology Industry Association, la Hong Kong Wireless Technology Industry Association, Nokia y ViVOtech.
- En febrero de 2007, Visa y SK Telecom anunciaron planes para lanzar el primer pago móvil sin contacto en el mundo, usando una SIM personalizada a través de la tecnología OTA. Esta solución está basada en la plataforma móvil de Visa. Este servicio inicialmente involucrará 30000 subscriptores de SK Telecom y 50000 puntos de venta.
- En febrero de 2007, Discover Financial Services y Motorola Inc. lanzaron una prueba de gestión de cuentas y pagos móviles que permitía a los participantes chequear los balances de su cuenta, revisar historiales de pago y hacer compras usando su teléfono celular en lugar de la tradicional tarjeta de crédito.

- En enero de 2007, Visa lanzo su plataforma móvil la cual pretende facilitar el desarrollo de servicios y pagos móviles. La plataforma es el resultado de una serie de pruebas globales y fue desarrollada con la participación de varios actores, entre los que se pueden destacar: CASSIS International, Nokia, Philips, IBM, VeriSign.

En la Tabla 1 se muestra una comparación de los diferentes proyectos mostrados.

Tabla 1. Comparación de diferentes sistemas de pago

PROYECTO	DISPOSITIVO	TECNOLOGIA DE ACCESO	CARACTERISTICAS
UPTF	- Teléfonos con soporte a J2ME - Dispositivo especialmente diseñado.	- WLAN - Red celular	- Basado en el protocolo SAS (*Secure Agreement Submission* – Acuerdo seguro de presentación) basado en PKI - Permite pago con bolsas de dinero, efectivo o crédito - El usuario debe digitar un PIN para autorizar el pago.
P2P	- Teléfonos con tecnología Bluetooth - Teléfonos con acceso a Internet	- Bluetooth - Internet inalámbrico	- Basado en el protocolo de seguridad P2P-Paid, basado en autenticación del usuario. - Permite pagos P2P - Basado en cuenta bancaria
PSP	- Dispositivos móviles con interfaz inalámbrica y acceso a Internet.	- LAN inalámbrica - WAN inalámbrica	- Basado en contratos de acuerdos a nivel de servicio entre el cliente y servidores - Basado en bolsas de dinero - Diseñado para micro pagos
PayPal	- Dispositivos móviles habilitados con WAP - Equipos de escritorio	- Internet	- Basados en cuentas - Sistema de pago remoto - Permite micro y macro pagos
MobyPay	- Teléfonos celulares	- Red celular	- Permite micro y macro pagos - La factura se puede cargar a la factura telefónica o a una cuenta - Permite pagos P2P o pagos en el punto de venta
SEMOPS	- Teléfonos celulares con acceso a internet a través de WAP	- Internet - Red celular	- Permite pagos P2P, pagos remotos y pagos en el punto de venta - Pagos a través del banco o del operador móvil. - Requiere la cooperación entre bancos y operadores móviles - Seguridad basada en la autenticación del usuario.
Pilotos NFC	- Dispositivos móviles con tecnología NFC inmersa	- NFC - OTA	- Sistemas de pago por proximidad - Diferentes opciones financieras (bolsas de dinero, tarjetas prepago, bancos) - Soluciones propietarias

Capítulo 2

PLATAFORMA DE FACTURACION Y PAGO DE SERVICIOS EN AMBIENTES MOVILES UBICUOS

La definición de la plataforma de facturación y pago se orienta a las características de los sistemas de pago en ambientes ubicuos definidas en el capitulo anterior.

Al ser una plataforma de pago, la seguridad se convierte en esencial, ya que sin ella los participantes en el servicio no se sentirán cómodos con su uso. La información que se transmite durante todo el proceso debe protegerse de intrusos debido a la naturaleza crítica de este tipo de información y además se deben definir políticas de seguridad adecuadas que garanticen la estabilidad, la eficiencia y el control de riesgos, condiciones indispensables en un sistema de pago y exigidos por cualquier entidad financiera involucrada.

Los sistemas de pago por proximidad tienen como característica principal la mínima intervención del usuario y la espontaneidad, lo que permite que el proceso de pago sea muy natural para el usuario y su ejecución en el punto de venta lo cual permite que los productos por los cuales el usuario está pagando, sean de toda índole y no solo servicios de descarga a través de la Web.

Otro factor importante en la caracterización del servicio es que su entorno de ejecución es Colombia, por lo cual debe adaptarse a las condiciones sociales, tecnológicas y legislativas del país. Por estas razones se ha determinado que la plataforma cumpla con las siguientes condiciones:

- Soporte a teléfonos celulares de gama baja y media que son los más comunes en Colombia.
- Por la anterior razón, la tecnología de contacto que se usa para adaptarse a este tipo de dispositivos es RFID en dispositivos de gama baja y media, y NFC en dispositivos de gama alta.
- Uso de certificados y firmas digitales como lo define la ley de comercio electrónico que existe en Colombia.

Para hacer más simple el servicio de pago para los usuarios, este se basa en cuentas bancarias y no en bolsas de dinero digitales, las cuales son menos comunes en Colombia, y a pesar de que el grado de bancarización en el país no es muy alto en algunos sectores, el gobierno está haciendo un gran esfuerzo por extenderlo.

En resumen, el Servicio de Facturación y Pago para ambientes ubicuos se desarrolló utilizando pagos por proximidad, brindando espontaneidad en el proceso y mínima intervención del usuario. Permite el pago de servicios ubicuos con un nivel alto de seguridad y privacidad brindando confianza a los usuarios. La seguridad de todo el sistema se maneja de forma distribuida, para no afectar la ubicuidad del sistema, y está basada en certificados digitales y claves de cifrado lo cual

brinda una mayor flexibilidad, garantiza la confidencialidad y la autenticación de la información y está acorde con la legislación Colombiana. Además, se puede accederse al servicio a través de cualquier dispositivo móvil, sin importar su gama, utilizando ya sea tecnología RFID o NFC, lo que permite su implantación en el contexto colombiano.

Basado en las características seleccionadas para la plataforma de facturación y pago, en este capítulo se presenta la descripción del servicio de facturación y pago y la arquitectura para llevar a cabo la implementación de la plataforma deseada.

2.1. Proceso de Facturación y Pago

Para acceder a la plataforma de facturación y pago, el usuario debe haber creado una cuenta de servicio en el sistema. En el momento en que esta es creada, se almacena en el dispositivo móvil la información necesaria para realizar pagos. La cuenta de servicio creada debe tener asociada una cuenta bancaria habilitada para pagos móviles de la cual finalmente se debitan los valores pagados por el usuario.

Antes de acceder a la plataforma de facturación y pago, el usuario debe haber accedido a un servicio ubicuo de compra y por tanto se asume que en su dispositivo móvil y en el punto de venta se encuentra la información de los artículos comprados y del valor a pagar. En este punto es importante aclarar que la plataforma propuesta, en este trabajo de grado, es responsable del proceso de facturación y pago y no del proceso de selección de los artículos y su compra.

En el momento de realizar el pago el usuario debe acercar su dispositivo móvil al lector que se encuentra en el punto de venta y de esta manera, sin ninguna otra intervención del usuario, el pago se hará efectivo.

Después de realizado el pago, el usuario recibe en su dispositivo móvil un mensaje de texto indicándole que este se realizó exitosamente, y la factura de la compra se le envía a través de un mensaje a la cuenta de correo electrónico, especificada por el usuario durante el proceso de subscripción al servicio.

En la Figura 2 se describe todo el proceso del servicio. Como se puede observar, en la plataforma de facturación y pago existen un gran número de partes involucradas, todas ellas relacionadas entre sí. A continuación se definen estas entidades que intervienen en el proceso y las relaciones entre ellas.

2.1.1. Roles

Dispositivo Móvil: corresponde al terminal del cliente, quien lo ha habilitado para realizar pagos. Debe tener dos interfaces de acceso, una de contacto basada en tecnología RFID o NFC, a través de la cual se hará efectivo el pago, y otra para una red de área amplia como GSM u otra tecnología celular, que permitirá el envío de mensajes de texto.

Punto de Venta: corresponde al sitio en donde el usuario hace efectivo el pago, debe contar con un dispositivo que permita leer los datos de la cuenta de servicio del usuario, almacenados en la etiqueta RFID o NFC. El punto de venta está asociado a un almacén o entidad que vende productos o servicios.

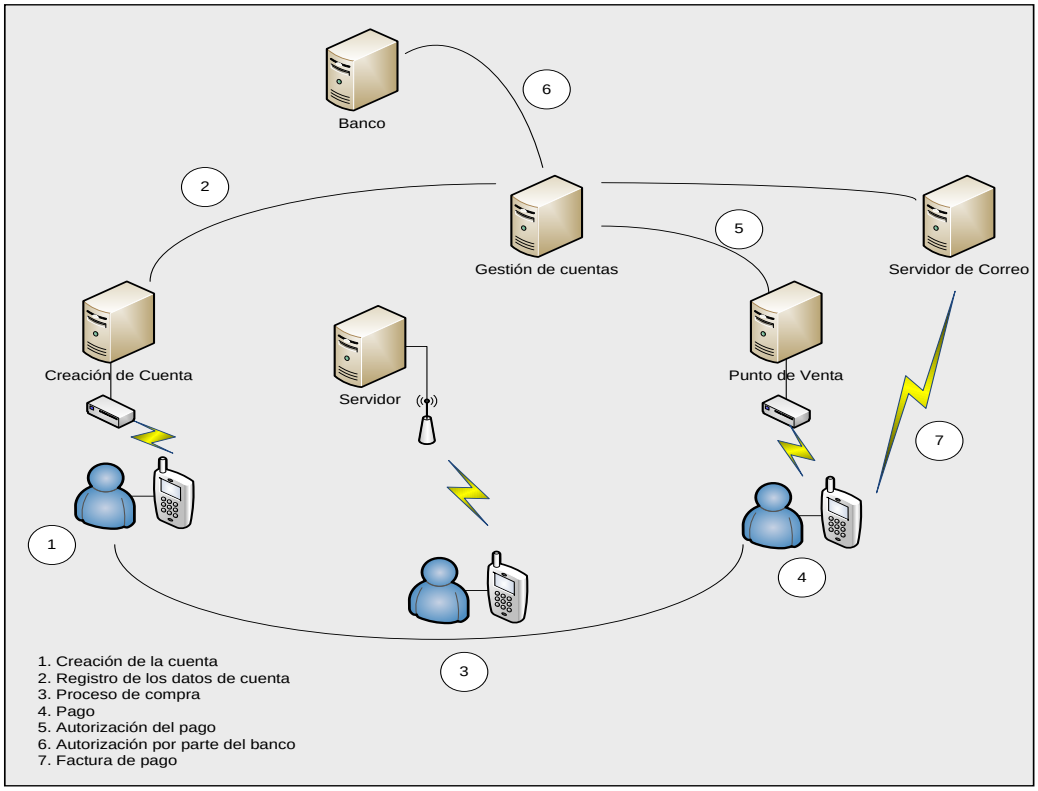


Figura 2.Proceso de Facturación y Pago

Administrador de Cuentas: pertenece a la compañía que presta el servicio de facturación y pago de servicios ubicuos, y se encarga de administrar las cuentas de servicio de los usuarios. Tiene como funciones crear las cuentas de servicio, generar a través de una autoridad de certificación las credenciales para el manejo de las cuentas y los pagos, asociar la cuenta de servicio a una cuenta bancaria, llevar registros del estado de las cuentas de servicio, modificar y cancelar las cuentas de servicio por solicitud del usuario, y pedir autorización a la entidad bancaria para hacer efectivas las transacciones realizadas por los usuarios.

Punto de Creación de Cuentas: asociado al Administrador de Cuentas, corresponde al punto a través del cual el usuario solicita la creación, bloqueo o eliminación de su cuenta de servicio. Debe contar con un dispositivo que permita leer y escribir en el elemento seguro (etiqueta NFC o RFID) del dispositivo móvil del usuario.

Proveedor de Mensajes: se encarga de enviar mensajes de notificación al dispositivo móvil, los cuales pueden generarse en el momento de creación de la cuenta de servicio, cuando la cuenta cambia de estado o cuando se realiza una transacción. También se encarga de enviar las facturas digitales generadas por sus compras.

Banco: encargado de la autorización del pago, dependiendo del estado de la cuenta bancaria del usuario.

Entidad Certificadora: se encarga de certificar la autenticidad de las entidades que intervienen en el proceso de pago, para ello les genera certificados y claves.

Certificador de la Factura Digital: entidad certificadora que proporciona un certificado para firmar digitalmente las facturas enviadas a los usuarios del servicio.

2.1.2. Relaciones

Dentro de todo el proceso para llevar a cabo el servicio de facturación y pago se establecen relaciones de tres tipos entre las entidades que hacen parte de la arquitectura:

1. Relaciones contractuales: representadas en contratos legales entre diferentes partes para proveer servicios y aceptar responsabilidades. La plataforma no administra directamente estos contratos pero asume que ellos existen.
2. Relaciones administrativas: deben ser establecidas antes de que el proceso de pago se lleve a cabo. Deben garantizar que todo el proceso se realice de manera correcta y segura.
3. Relaciones operacionales: son de corta duración y tienen lugar cuando se está efectuando un pago.

En la Figura 3 se muestran las relaciones contractuales:

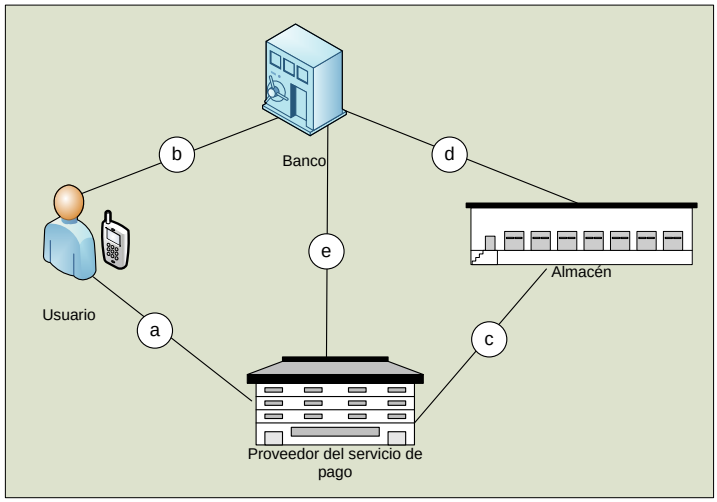


Figura 3. Relaciones Contractuales

a) El dueño del dispositivo móvil debe establecer un contrato con la compañía prestadora del servicio de facturación y pago, en donde se definen claramente las responsabilidades de cada una de las partes.

   Las responsabilidades del cliente son:

   - Informar cualquier problema con el dispositivo (robo, pérdida, daño, entre otros).
   - Crear una cuenta bancaria que permita hacer pagos móviles e inscribirla en el momento de creación de la cuenta de servicio.

   Las responsabilidades de la compañía prestadora del servicio de facturación y pago son:

   - Administrar de manera segura la cuenta de servicio del usuario.
   - Mantener segura toda la información relacionada con el cliente.

- Enviar la información de las transacciones del usuario al banco respectivo, de manera segura y bajo el esquema que este defina.

b) El dueño del dispositivo móvil debe tener una cuenta habilitada para pagos móviles con el banco. Las responsabilidades de cada uno de ellos deberán estar bien especificadas.

Las responsabilidades del cliente son:

- Cumplir con todos los requerimientos exigidos por el banco para el manejo de las cuentas bancarias.

Las responsabilidades del banco son:

- Hacer un manejo seguro de todas las transacciones hechas por el cliente
- Habilitar la cuenta para el pago a través de dispositivos móviles
- Informar al cliente de las transacciones realizadas

c) El dueño del punto de venta (almacén) debe establecer un contrato con la compañía prestadora del servicio de facturación y pago.

Las responsabilidades de la compañía prestadora del servicio de facturación y pago son:

- Informar al banco acerca de las transacciones hechas por el cliente para que los valores sean debitados de su cuenta y transferidos a la del almacén.
- Garantizar la seguridad en todos los procesos de transferencia de información.

Las responsabilidades del punto de venta (almacén) son:

- El almacén se compromete a pagar un importe a la compañía prestadora del servicio de facturación y pago por el servicio recibido.

d) El dueño del punto de venta debe tener una cuenta con el banco.

Las responsabilidades del punto de venta (almacén) son:

- Cumplir con todos los requerimientos exigidos por el banco para el manejo de las cuentas bancarias.

Las responsabilidades del banco son:

- Hacer un manejo seguro de todas las transacciones realizadas por el almacén.
- Habilitar la cuenta para recibir consignaciones debitadas de cuentas habilitadas para pagos a través de dispositivos móviles.
- Informar al almacén de las transacciones realizadas.

e) La compañía prestadora del servicio de facturación y pago debe establecer un contrato con el banco para el manejo de las cuentas para pagos móviles y para la autorización de las transacciones.

Las responsabilidades de la compañía prestadora del servicio de facturación y pago son:

- Cumplir con todos los requerimientos exigidos por el banco para poder realizar las transacciones de los clientes del servicio.

Las responsabilidades del banco son:

- Manejar de forma segura todas las transacciones hechas por el servicio de pago.

En la Figura 4 se muestran las relaciones administrativas.

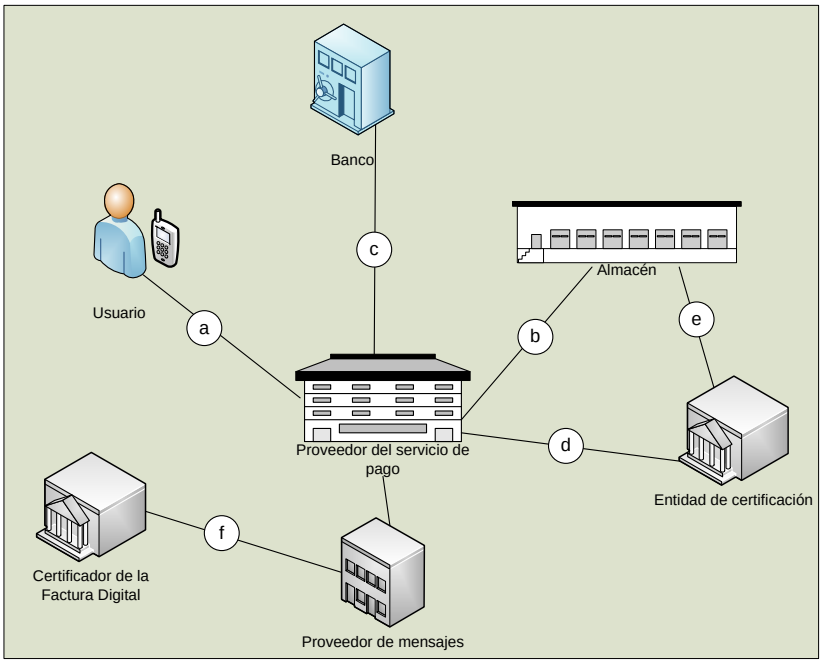


Figura 4. Relaciones Administrativas

a) El usuario establece una relación con la compañía prestadora del servicio de facturación y pago, para obtener una cuenta e instalar en el elemento seguro (etiqueta RFID/NFC) la información de la cuenta y de las credenciales que le permitan realizar los pagos a través de su dispositivo móvil. Para el caso de dispositivos NFC también debe instalarse una aplicación que le permita realizar el pago.

b) La compañía prestadora del servicio de facturación y pago debe establecer una relación con el almacén dueño del punto de venta (POS) a través del cual el usuario realiza los pagos. La compañía prestadora del servicio de facturación y pago debe instalar en el punto de venta el software necesario para realizar todos los procesos requeridos para finalizar una transacción comercial.

c) La compañía prestadora del servicio de facturación y pago tiene una relación con el Banco a través de una interfaz por medio de la cual se debe enviar toda la información de las

transacciones para que éste pueda debitar los valores de las cuentas de los usuarios y transferirlas a la del almacén. En la interfaz se deben implementar todas las condiciones de seguridad exigidas por el banco para el establecimiento de la relación.

d) La compañía prestadora del servicio de facturación y pago tiene una relación con la autoridad de certificación, la cual debe garantizar la legitimidad de esta entidad ante el resto de las partes involucradas en el proceso de facturación y pago, a través de la generación de los certificados y de las claves respectivas.
e) El punto de venta tiene una relación con la autoridad de certificación, por medio de la cual a través de la autoridad de certificación se garantiza la autenticidad del punto de venta.
f) El proveedor de mensajes se relaciona con el certificador de la factura digital, el cual le permite firmar los mensajes que contienen la factura de la compra a enviar al usuario. Los mensajes se firman usando un certificado digital entregado por la entidad certificadora.

En la Figura 5 se muestran las relaciones operacionales.

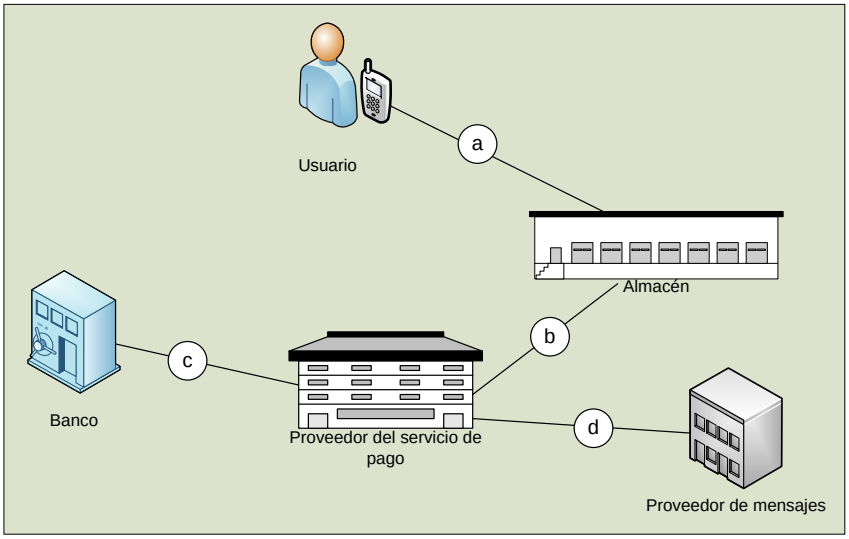


Figura 5. Relaciones Operacionales

a) El usuario establece una relación con el punto de venta del almacén, a través de la interfaz de contacto RFID/NFC de su dispositivo móvil. Esta relación debe ser segura, ya que a través de ella el usuario envía las credenciales, las cuales se encuentran almacenadas en el elemento seguro del dispositivo móvil (etiqueta RFID/NFC)
b) El punto de venta del almacén tiene una relación con el administrador de cuentas, a través de la cual se realiza la verificación de la información de la cuenta del usuario y los datos de la compra y se pide la autorización para realizar el pago a través de la misma. El envío de toda la información entre estas entidades se debe hacer de manera segura.
c) El administrador de cuentas establece una relación con el banco, con el fin de enviarle la información de la cuenta y el valor a debitar, relacionada con el cliente que hizo un pago a través de su dispositivo móvil.
d) El administrador de cuentas establece relaciones con el proveedor de mensajes para solicitar el envío de mensajes de información y la factura al usuario.

2.2. Requerimientos de la Plataforma de Facturación y Pago

Teniendo en cuenta la descripción de la plataforma y las características del servicio de facturación y pago, se pueden determinar los requerimientos de la misma, los cuales se muestran en la Tabla 2.

Tabla 2. Requerimientos de la Plataforma de Facturación y Pago

FUNCIONALES	Asociados a la cuenta de servicio	Crear una cuenta de servicio
		Asociar una cuenta bancaria a la cuenta del servicio
		Almacenar las credenciales del usuario en el elemento seguro del dispositivo móvil
		Almacenar la información del usuario y las credenciales en el sistema
		Modificar la cuenta de servicio del usuario
		Borrar la cuenta de servicio de usuario (y las credenciales del elemento seguro)
		Informar al usuario el resultado de las acciones solicitadas
	Asociados al pago	Activar el pago, a través de una interfaz en el dispositivo móvil
		Hacer efectivo el pago al acercar el dispositivo móvil al lector del POS
		Enviar la información del pago al banco para su autorización
		Informar al usuario a través de un mensaje el resultado del proceso
	Asociados a la facturación	Enviar la factura digital al correo electrónico indicado por el usuario en el momento de crear la cuenta
NO FUNCIONALES	Seguridad	
	Privacidad	
	Mínima intervención del usuario	
	Espontaneidad	
	Eficiencia	
	Flexibilidad	
	Despliegue	

En la Tabla 3 se destacan las características más importantes de la plataforma, que la hacen diferente a los proyectos y sistemas existentes.

Tabla 3. Características de la Plataforma de Facturación y Pago

PROYECTO	DISPOSITIVO	TECNOLOGIA DE ACCESO	CARACTERISTICAS
PLATAFORMA DE FACTURACION Y PAGO	- Teléfonos celulares con etiquetas RFID - Teléfonos celulares con tecnología NFC inmersa.	- RFID/NFC - Red celular (SMS) - Internet	- Seguridad basada en certificados digitales y criptografía. - Sistema de pago espontáneo - Pago por proximidad en el punto de venta - Basados en cuentas de servicio - Asociado a cuenta bancaria - Envío de facturas digitales

2.3. Arquitectura de Facturación y Pago

Como se infiere de los apartados anteriores, la plataforma de facturación y pago es bastante compleja ya que debe cumplir con varios requerimientos y además aparecen involucrados una gran cantidad de actores con diversos tipos de relaciones entre ellos. Es por esta razón que se decidió adoptar para su desarrollo, un análisis basado en Arquitecturas de Software, disciplina que ha resultado de la evolución de la Ingeniería de Software para atacar problemas de gran envergadura permitiendo la integración de aplicaciones y sistemas de información en las organizaciones [36].

La Arquitectura se definió usando el Patrón de Arquitectura en Capas, en donde la estructura de las aplicaciones puede ser descompuesta en grupos de sub-tareas que se encuentran en un determinado nivel de abstracción. Este patrón fue escogido por las grandes ventajas [37] que ofrece:

- Al estar basado en niveles de abstracción crecientes permite la división de un problema complejo en una secuencia de pasos incrementales.
- Al tener los componentes de cada capa el mismo nivel de abstracción, se facilita la reutilización ya que se pueden emplear varias versiones de una misma capa siempre y cuando mantengan las mismas interfaces hacia las capas adyacentes.
- Debido a que las especificaciones de una capa no dicen nada sobre su implementación, los detalles de esta se ocultan a las otras, lo cual facilita el diseño de la plataforma.

Con base en la caracterización de la plataforma de facturación y pago y de sus requerimientos, se definieron unas sub-tareas con el fin de definir la estructura de la arquitectura:

- Creación de las cuentas de usuario.
- Manejo y administración de las cuentas del servicio de facturación y pago.
- Almacenamiento y administración de la información de los usuarios.
- Interfaz con el banco.
- Pago de los productos.
- Envío de mensajes informativos al usuario.
- Envío de la factura digital al usuario.
- Certificación de los participantes en el proceso.
- Firma digital de la factura.

Cada una de las tareas definidas se asoció a un módulo funcional dentro de la arquitectura, quedando la estructura como se muestra en la Figura 6. La descripción de cada uno de los módulos y la información que se transmiten entre ellos, se presenta a continuación:

- **Dispositivo Móvil**: es la parte correspondiente al lado cliente de la arquitectura. A través de este módulo, el usuario interactúa con la plataforma de pago y es aquí donde se almacena la información de las credenciales de la cuenta del usuario. Esto se debe hacer en el elemento seguro del dispositivo (etiqueta RFID/NFC). Establece comunicación con el Punto de Creación de la Cuenta, y es en este momento cuando se almacenan las credenciales en su elemento seguro. Cuando se va a efectuar el pago, se comunica con el Punto de Venta, quien se encarga de leer las credenciales almacenadas.

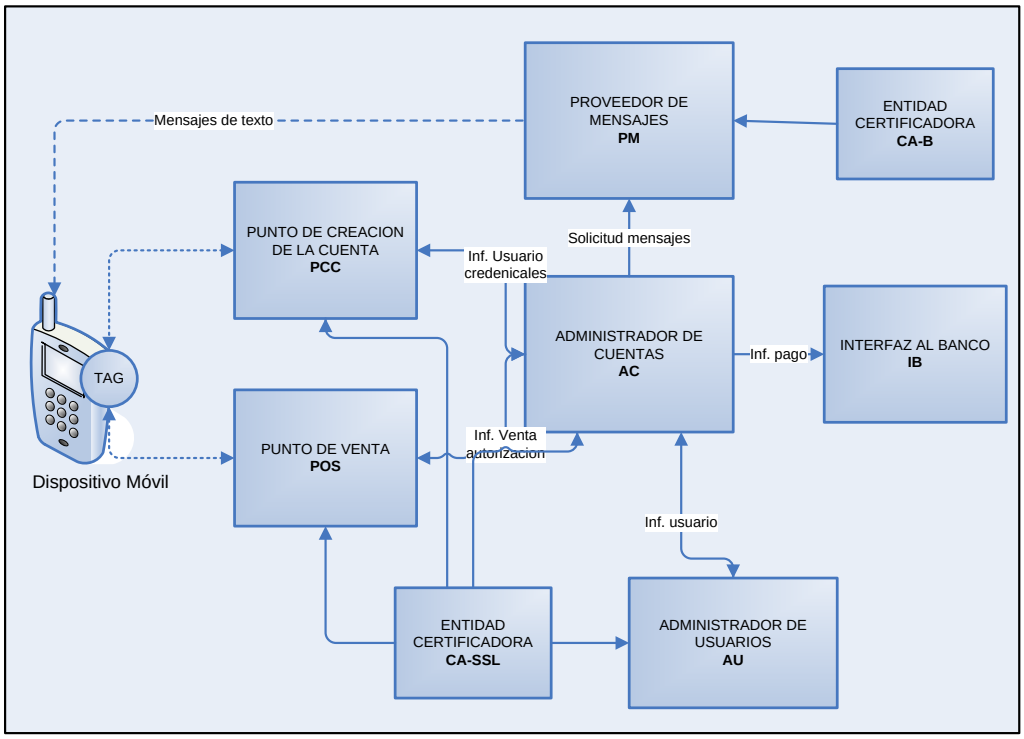


Figura 6. Arquitectura General de Facturación y Pago

- **Punto de Venta**: es el módulo a través del cual el usuario hace efectivo el pago, lee las credenciales almacenadas en el dispositivo móvil y las transfiere hacia el Administrador de Cuentas.
- **Punto de Creación de la Cuenta**: a través de este módulo el usuario se inscribe al servicio de facturación y pago, y puede realizar funciones como crear una cuenta para la realización de los pagos, bloquearla en caso de robo del dispositivo móvil o cancelarla cuando no quiera más el servicio. Este módulo envía la información del usuario al Administrador de Cuentas y recibe de este las credenciales, las cuales envía al dispositivo móvil para su almacenamiento.
- **Administrador de Cuentas:** es uno de los módulos más importantes de la arquitectura ya que establece comunicación con la mayoría de ellos. Coordina todo el proceso de autenticación y autorización, genera las credenciales del usuario, las cuales están conformadas por la identificación del usuario y la clave asociada, y las envía al Punto de Creación de la Cuenta para que sean almacenadas en el elemento seguro del dispositivo móvil. Toda la información relacionada con el usuario y la cuenta de servicio la envía al modulo Administrador de Usuarios para su almacenamiento. En el momento del pago, recibe la información de las credenciales del usuario del Punto de Venta y se comunica con el banco a través de la Interfaz respectiva y con el Administrador de Usuarios para solicitar la autorización del pago.
- **Administrador de Usuarios**: este módulo se constituye en el repositorio de los datos relacionados con la información de los usuarios y sus credenciales, que permiten la validación de la identidad de los usuarios en el momento de realización del pago.
- **Interfaz al Banco**: este módulo permite la interacción del modulo Administrador de Cuentas con el banco que ofrece a los usuarios las cuentas bancarias habilitadas para pagos móviles. Debe implementar las condiciones de seguridad exigidas por el banco, así que en su mayoría depende de las características de esta entidad más que de la propia plataforma de facturación y pago.

- **Proveedor de Mensajes**: es el encargado de enviar mensajes al dispositivo móvil del usuario, a solicitud del Administrador de Cuentas. Los mensajes que se envían al usuario son mensajes de confirmación de realización de un servicio, ya sea con respecto a la cuenta o al pago. Este módulo también se encarga del envío de la factura digital al usuario a la cuenta de correo definida por el usuario en el momento de creación de la cuenta del servicio de facturación y pago.

2.4. Características de la Arquitectura

La Arquitectura de Facturación y Pago se constituye en la materialización de la plataforma de facturación y pago definida en los apartados anteriores, por tal razón y teniendo en cuenta los requisitos de la plataforma descritos en el numeral 2.2 y las particularidades de la plataforma mostradas en la Tabla 2, se definen las características de la arquitectura las cuales se describen a continuación.

2.4.1.Seguridad

Los aspectos tenidos en cuenta durante la definición de la arquitectura asociados a la seguridad son los siguientes:

Confidencialidad

Las credenciales de la cuenta del usuario permanecen seguras durante todo el proceso, tanto de creación de la cuenta como del pago. Esto implica que se garantiza la confidencialidad mientras estos datos permanecen almacenados en el dispositivo móvil y cuando ellos viajan a través de las diferentes redes en el momento en que se realiza el proceso de pago.

En el momento de la creación de la cuenta de servicio, el Administrador de Cuentas genera las credenciales asociadas al usuario y su cuenta las cuales se almacenan en el elemento seguro del dispositivo móvil, esta información es enviada al Punto de Venta de manera cifrada. El proceso de envío de esta información desde el Punto de Venta hacia el elemento seguro del dispositivo móvil se realiza utilizando un algoritmo seguro.

Durante el proceso de pago, la información de las credenciales del usuario contenidas en la etiqueta del dispositivo móvil, se envían al lector a través del mismo algoritmo seguro usado durante la creación de la cuenta, esta información también se envía al Administrador de Cuentas de manera cifrada.

Para que el pago se haga efectivo se envía información al banco, a través de la interfaz desarrollada para este fin, esta información se transmite usando el protocolo de seguridad definido por el banco.

Autenticación

Durante todo el proceso de pago se debe garantizar la autenticidad de las entidades que intervienen en el mismo, de esta manera se impide que información sensible, como las

credenciales del usuario, quede expuesta a personas mal intencionadas. Las entidades que deben autenticarse son:

- El dispositivo móvil que contiene la etiqueta RFID: esta autenticación la debe garantizar el Administrador de Cuentas a través de la identificación de las credenciales contenidas en la etiqueta.
- El Administrador de Cuentas: el almacén que posee el punto de venta habilitado para pagos ubicuos, debe estar seguro que el Administrador de Cuentas con el cual va a establecer una comunicación, es quien dice ser. Esto se logra a través de la entidad certificadora asociada a el, la cual debe generar los certificados que permiten realizar esta validación. El Administrador de Cuentas también debe autenticarse frente al banco, esto se hace también utilizando certificados digitales.
- El proveedor de mensajes: el usuario debe estar seguro que la factura recibida en su correo electrónico es válida. Esto se hace a través del certificado digital generado por la entidad certificadora asociada al proveedor de mensajes, el cual genera la firma digital asociada al mensaje y garantiza la procedencia del mismo.

Autorización

Se debe garantizar que tanto los usuarios como las entidades participantes en el proceso del pago y facturación tienen los permisos adecuados para realizar las acciones que intentan ejecutar, asegurando de esta manera que la información solo sea manipulada por las personas y entidades adecuadas, salvaguardando los datos sensibles del proceso. La autorización se realiza en el contexto de la autenticación. En el momento en que los participantes se autentican de manera satisfactoria se les permite seguir con los procesos iniciados, en caso de que la autenticación falle se generan mensajes de error y se realiza la interrupción de los mismos.

No repudio

La utilización de los certificados digitales y la criptografía de claves públicas para "firmar" las transacciones y los mensajes se constituyen en pruebas de las transacciones llevadas a cabo. La firma digital de los datos es una prueba suficiente. Esta característica les garantiza a los usuarios que la factura digital proviene de la entidad adecuada y que será válida como prueba de su compra, al igual que una factura normal.

Proceso de Certificación

El proceso de certificación dentro de la Arquitectura de facturación y pago permite que los módulos que deben transferir información sensible puedan autenticarse frente a los otros y de esta manera garantizar su autenticidad. Además, permite que la generación de las claves para cifrar los mensajes se realice también de manera segura.

En la arquitectura de facturación y pago los módulos que requieren certificados digitales para poder realizar procesos de autenticación son: Administrador de Cuentas, Administrador de Usuarios, Punto de Venta y Punto de Creación de la Cuenta.

Estos certificados digitales serán emitidos para la autoridad de certificación CA-SSL.

Por otro lado el emisor de mensajes requiere de una firma digital, para garantizar la autenticidad de las facturas digitales enviadas al usuario. Esta firma será generada por la autoridad de certificación CA-B.

Transferencia de Mensajes Seguros

La transferencia de información entre los módulos de la arquitectura se hace de manera segura, utilizando técnicas de criptografía de la siguiente manera:

- Entre el elemento seguro del dispositivo móvil y el Punto de Creación de la Cuenta/Punto de Venta. Los mensajes que se transfieren entre estos dos bloques se cifran a través de una algoritmo seguro propietario establecido entre la etiqueta ubicada en el dispositivo móvil y el lector presente en el Punto de Creación de la Cuenta/Punto de Venta.
- Entre el Punto de Creación de la Cuenta/Punto de Venta y el Administrador de Cuentas. Los mensajes que se transfieren entre este par de módulos se cifran usando técnicas criptográficas que combinan tanto cifrado simétrico como asimétrico, usando para ello las claves generadas por la autoridad de certificación.
- Entre el Administrador de Cuentas y el Administrador de Usuarios: La información transferida entre estos módulos se cifra usando las claves generadas por la autoridad de certificación.

Entre el administrador de cuentas y la Interfaz al Banco: La información transferida entre estos módulos se cifra con base en la información entregada por la autoridad de certificación definida entre las partes.

2.4.2. Privacidad.

La privacidad dentro la arquitectura se logra almacenando los datos del usuario y su cuenta en el elemento seguro del dispositivo móvil. Además, toda esa información viaja cifrada durante cualquier transmisión, como se explicó en el apartado anterior.

La privacidad de los datos de los usuarios se conserva siempre ya que las personas sin una cuenta de servicio no pueden acceder a la información de ningún usuario, los clientes del servicio podrán leer la información de su cuenta pero no realizar cambios sobre ella, y el administrador en caso de ser necesario, debe acceder a la información de los usuarios a excepción de aquella previamente cifrada.

La información del usuario y su cuenta solamente es utilizada por la arquitectura en el momento de realizar el pago y no está disponible para ningún otro proceso.

2.4.3. Mínima intervención del usuario

En la arquitectura de facturación y pago toda la información del usuario, necesaria para efectuar el pago, se almacena en el elemento seguro del dispositivo móvil (etiqueta RFID/NFC) de esta manera en el momento de efectuar el pago el sistema no pide digitar claves ni realizar confirmaciones, este hecho hace que el sistema de pago sea natural y requiera la mínima intervención por parte del usuario, por otro lado, en el caso de NFC, las aplicaciones que se

implementan sobre el dispositivo son simples y livianas dadas las capacidades de los dispositivos móviles en cuanto a despliegue, memoria y procesamiento.

2.4.4. Espontaneidad

La arquitectura de facturación y pago permite que los usuarios puedan iniciar el proceso de pago en cualquier momento, en los puntos de venta habilitados, una vez han creado una cuenta en el sistema. El proceso de pago es corto debido a las propiedades de las tecnologías y herramientas empleadas, por lo cual es poco probable que el cliente establezca una relación de larga duración con el sistema durante el proceso de pago, convirtiéndolo en un sistema con tiempos de transacción comparables a los de sistemas de pago tradicionales como el de tarjetas débito o de crédito.

2.4.5. Eficiencia

La eficiencia de la arquitectura se mide en el tiempo que dura la transacción. El proceso de pago se lleva a cabo simplemente pasando el dispositivo móvil cerca al lector ubicado en el punto de venta. Los mensajes de confirmación del pago se envían a través de la red celular y sus tiempos de llegada dependen de la congestión en dichas redes y de si los dispositivos se encuentran en zonas de cobertura, por esta razón estos tiempos no se tienen en cuenta para medir la eficiencia del sistema de pago.

2.4.6. Flexibilidad

La arquitectura de facturación y pago es flexible comparada frente a otras formas de pago tradicionales, el sistema permite el funcionamiento en situación de desconexión del dispositivo móvil a la red celular, ya que independiente de esto, el pago se podrá realizar en un punto de venta y solo se afecta el tiempo de recepción de los mensajes de notificación.

La flexibilidad también se aprecia en el hecho de que mediante el uso de la plataforma se pueden realizar macro pagos y micro pagos, aunque su concepción se hizo teniendo en cuenta las condiciones requeridas para los micro pagos. Para la realización de macro pagos, dada el monto de los pagos a realizar, se debe agregar un esquema adicional de verificación, como la presentación del algún documento de identidad del usuario en el momento de realizar el pago.

2.4.7. Despliegue

Dadas las condiciones bajo las cuales se desarrolla la arquitectura de facturación y pago el proceso de ampliar la cobertura del servicio es bastante sencillo, la creación de nuevos puntos de pago y de nuevas cuentas de usuario no implica la modificación de la arquitectura, para dar soporte a esta característica durante la implementación de la arquitectura se utilizaron herramientas robustas de desarrollo.

La arquitectura facilita la incorporación e interacción del sistema con otros servicios, gracias a la flexibilidad e interoperabilidad que ofrece el diseño en capas, de esta forma la plataforma queda abierta a posibles mejoras, modificaciones y nuevas aplicaciones que complementen u optimicen el proceso de pago.

Capítulo 3

DISEÑO DE LA PLATAFORMA DE FACTURACION Y PAGO

3.1. Modelo en Capas de los componentes de la Arquitectura de Facturación y Pago.

Para el diseño de cada uno de los componentes de la arquitectura de facturación y pago se adoptó el modelo de n-capas el cual se caracteriza por la descomposición funcional de las aplicaciones, de los componentes del servicio y su despliegue de forma distribuida, mejorando la escalabilidad, disponibilidad, gestión y utilización de recursos. Cada capa representa un componente separado en hardware o en software que ejecuta una función específica [38].

La aproximación más común del modelo, es el de 3 capas, el cual consta de capa de presentación, capa de lógica del negocio y la capa de datos, La capa de presentación generalmente es una interfaz de usuario grafica que despliega datos a los usuarios sin importar el tipo de dispositivo o su ubicación y le permite la manipulación de la información; la capa de lógica del negocio controla la funcionalidad de la aplicación ejecutando procesamiento detallado [39] y la capa de datos permite el almacenamiento y la recuperación de la información independiente de la lógica del negocio.

Dos aspectos importantes dentro de la arquitectura son la seguridad y la eficiencia en el manejo de los datos, tanto en su manipulación como en su transmisión, por ello además de las capas mencionadas, dentro del diseño se incluyeron: la capa de acceso a datos, la capa de comunicación y la capa de seguridad.

A nivel general, la función de cada una de las capas propuestas se describe a continuación.

- La **Capa de Presentación** contiene interfaces hacia los diferentes usuarios del sistema. El cliente, en el dispositivo móvil, el vendedor en el punto de venta y para el administrador del sistema (quien ingresa los datos del usuario en el punto de creación de la cuenta).
- En la **Capa de Lógica del Negocio** se ejecutan todas las acciones que se deben llevar a cabo para la realización de los procesos de pago y facturación. Esta capa recibe los datos de la capa de presentación, los procesa de acuerdo a los requerimientos del sistema, y entrega, de nuevo a la capa de presentación, los datos que deben ser visualizados por el usuario.
- La **Capa de Acceso a Datos** contiene todas las funciones necesarias para que los datos relacionados con la información del usuario y su cuenta se puedan consultar y escribir en los repositorios correspondientes.

- La **Capa de Datos** representa el repositorio de los datos relacionados con el usuario y su cuenta.
- La **Capa de Seguridad** se encarga del manejo seguro de toda la información que se procesa en el sistema, garantizando la autenticación, la integridad, la confidencialidad y el no repudio de los datos. Para ello se cifra toda la información relacionada con el usuario y su cuenta, y se garantiza la autenticidad de las partes que intervienen en el proceso de facturación y pago, a través de autoridades de certificación.
- La **Capa de Comunicaciones** representa a todos los protocolos de comunicación utilizados entre los diferentes módulos de la arquitectura para la efectiva transmisión de los datos. Toda la información sensible que debe ser transportada entre diferentes módulos se envía utilizando protocolos de comunicación seguros o firmada digitalmente

A continuación se muestra la descripción detallada de cada uno de los módulos que conforman la arquitectura de facturación y pago, las capas que los conforman y la función de cada una de ellas.

3.1.1. Dispositivo móvil

A través de este módulo el usuario interactúa con el servicio de pago y es aquí donde se almacena la información de las credenciales de la cuenta del usuario. Esto se hace en el elemento seguro del dispositivo (etiqueta RFID/NFC).

Cuando la tecnología de contacto que se usa es RFID no se requieren la capa de presentación ni la capa de lógica del negocio, ya que la etiqueta RFID es totalmente independiente del dispositivo y por tanto las aplicaciones que residen dentro del mismo no pueden acceder a la información almacenada en la etiqueta.

A diferencia de RFID, la tecnología NFC viene integrada dentro del móvil, lo que le permite al usuario acceder fácilmente a servicios o realizar operaciones en las distintas funciones de su dispositivo. Esto también permite desarrollar aplicaciones de valor agregado dentro del dispositivo para que interactúen con los datos almacenados en la etiqueta.

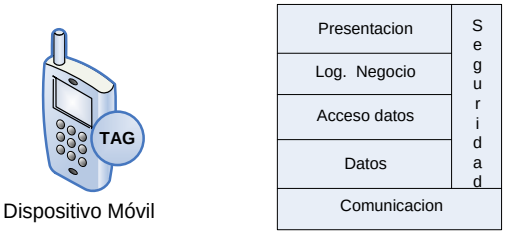


Figura 7. Dispositivo Móvil

- **Capa de presentación**. Contiene interfaces hacia el usuario del servicio, a través de las cuales éste, en el momento en que termina de seleccionar los productos que desea comprar, activa el pago (cuando la tecnología de contacto es NFC). También, a través de esta capa el usuario recibe los mensajes que le indican el resultado de las acciones relativas al servicio de facturación y pago.
- **Capa de Lógica del Negocio**. Soporta las funciones necesarias para el procesamiento de la información almacenada en el elemento seguro del dispositivo móvil, cuando la tecnología de contacto es NFC. Cuando la tecnología es RFID esta capa no existe.

- **Capa de Acceso a Datos**. Contiene funcionalidades que permiten leer y escribir en la etiqueta RFID (elemento seguro).
- **Capa de Datos**. Representa el repositorio de los datos del lado del cliente.
- **Capa de Seguridad**. Se encarga de garantizar que el acceso a la información almacenada en el elemento seguro del dispositivo móvil (etiqueta RFID) se haga de forma segura, a través del uso de técnicas de cifrado, y solo por el lector adecuado garantizando de esta manera la confidencialidad de los datos , la autorización y autenticación mutua.
- **Capa de Comunicación**. Se encarga del establecimiento de la comunicación entre la etiqueta RFID y el lector ubicado ya sea en el módulo de Punto de Venta o en el Punto de Creación de la Cuenta, esta comunicación se realiza a través del uso del protocolo estandarizado para las comunicaciones sin contacto ISO 14443B, lo cual permite el uso de las tecnologías RFID o NFC.

3.1.2. Punto de Venta

El Punto de Venta es el módulo a través del cual el usuario hace efectivo el pago, acercando el dispositivo móvil al lector de contacto cercano respectivo (RFID, NFC). En la Figura 8 se muestran las capas que lo conforman.

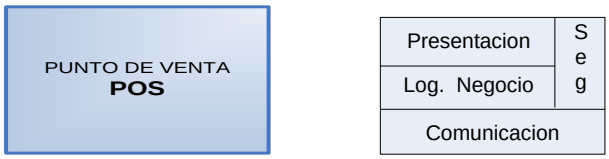


Figura 8. Punto de Venta

- **Capa de Presentación**. Contiene una interfaz gráfica que permite al vendedor visualizar las interacciones con el módulo Administrador de Cuentas y conocer el resultado de las operaciones realizadas. También a través de esta interfaz, el punto de venta se registra en la plataforma de facturación y pago.
- **Capa de Lógica del Negocio.** Verifica que la información enviada por el dispositivo móvil sea válida, además coordina todo el proceso de acceso al modulo Administrador de Cuentas y determina si la información de las credenciales del usuario deben ser enviadas o no a dicho módulo.
- **Capa de Seguridad**. Se encarga de garantizar que la comunicación con la etiqueta ubicada en el dispositivo móvil se haga de manera segura, para ello se utilizan mecanismos de seguridad propietarios de los fabricantes de las etiquetas y los lectores. También garantiza la seguridad en la comunicación con el Administrador de Cuentas mediante mecanismos de certificación procurando de esta manera que usuarios no autorizados tengan acceso a dicho módulo.
- **Capa de Comunicación**. Contiene todas las funciones necesarias para hacer efectiva la comunicación con el dispositivo móvil y el Administrador de Cuentas. Con el dispositivo móvil se comunica a través del lector de las etiquetas RFID ubicado en el punto de venta, esta comunicación se codifica utilizando un algoritmo seguro predefinido por el fabricante. Por otro lado, la comunicación con el módulo Administrador de Cuentas se hace utilizando el protocolo SOAP (*Simple Object Acces Protocol* – Protocolo Simple de Acceso a Objetos) sobre HTTPS (*HiperText Transfer Protocol Secure* – Protocolo Seguro de Transferencia de Hipertexto) que garantiza la seguridad de la información.

3.1.3. Punto de Creación de la Cuenta

A través de este módulo, el usuario se inscribe al servicio de facturación y pago, y puede realizar funciones como crear una cuenta para la realización de los pagos, bloquearla en caso de robo del dispositivo móvil o cancelarla cuando no quiera más el servicio.

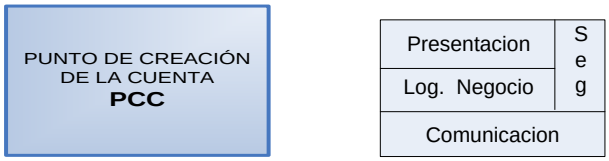


Figura 9. Punto de Creación de la Cuenta

- **Capa de Presentación**. Presenta la interfaz que le permite al administrador de las cuentas, el ingreso de los datos del usuario necesarios para la creación de la cuenta del servicio de facturación y pago, el bloqueo de la misma cuando la solicite el usuario y su eliminación cuando se cancele el servicio.
- **Capa de Lógica del Negocio**. Recibe la información del usuario, verifica que esté completa y la envía al módulo Administrador de Cuentas. Este módulo le retorna la información de las credenciales del usuario que deben ser almacenadas en la etiqueta del dispositivo móvil.
- **Capa de Seguridad**. Tiene las mismas funciones que la capa de seguridad del módulo de Punto de Venta.
- **Capa de Comunicación**. Tiene las mismas funciones que la capa de comunicación del módulo Punto de Venta.

3.1.4. Administrador de Cuentas

El Administrador de Cuentas es un bloque muy importante de la arquitectura ya que coordina algunas funciones de los otros módulos y por tanto establece comunicación con la mayoría de ellos. Gestiona todo el proceso de autenticación y autorización, genera las credenciales del usuario que deben ser almacenadas en el elemento seguro de su dispositivo móvil, todo esto lo hace a través de la autoridad de certificación CA-SSL.

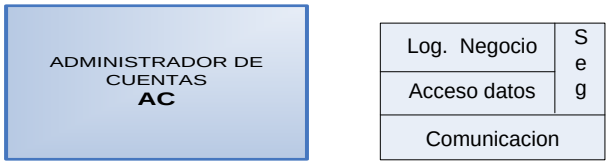


Figura 10. Administrador de Cuentas

- **Capa de Lógica del Negocio**. Las funciones de esta capa son.
  - Recibir los datos del usuario desde el Punto de Creación de la Cuenta y generar los identificadores y las claves para cada uno de ellos a través de la entidad de certificación CA-SSL.
  - Administrar las cuentas de los usuarios, crearlas, modificarlas y borrarlas a solicitud del Punto de Creación de Cuentas.

- Verificar las credenciales del usuario, enviadas por el Punto de Pago, a través de una consulta al Administrador de Usuarios.
- Recibir la información del pago y enviarla a la Interfaz del Banco para que se autorice el pago.
- Generar la información de los mensajes de texto y de la factura digital y solicitar su envío al módulo Proveedor de Mensajes.

- **Capa de Acceso a Datos**. Permite el acceso a los datos almacenados tanto en el módulo Administrador de Usuarios, como en las bases de datos del banco.
- **Capa de Seguridad**. Se encarga de verificar, a través de los certificados digitales, la identidad de los módulos con los que se comunica. Debe cifrar la información que se envía a los módulos con los que se establece comunicación, a través del uso de claves generadas por la autoridad de certificación CA-SSL.
- **Capa de Comunicación**. Contiene las funciones necesarias para hacer efectiva la comunicación con los módulos Punto de Venta y Punto de Creación de la Cuenta, la cual se basa en el protocolo de comunicación seguro SOAP sobre HTTPS. También permite la comunicación con la Interfaz al Banco y con el Proveedor de Mensajes.

3.1.5. Administrador de Usuarios

Este módulo se constituye en el repositorio de los datos relacionados con la información de los usuarios y sus credenciales, que permiten la validación de la identidad de los usuarios en el momento de realización del pago.

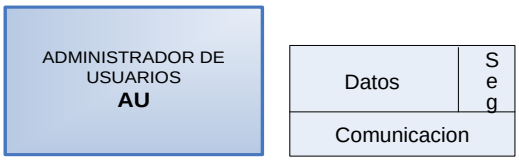


Figura 11. Administrador de Usuarios

- **Capa de Datos**. Se encarga de almacenar los datos relativos a los usuarios del servicio, como son la información personal, los datos de la cuenta y las credenciales generadas por el Administrador de Cuentas.
- **Capa de Seguridad**. Se encarga de verificar la identidad del Administrador de Cuentas, a través del certificado digital. Además, cifra la información que este le envía a través de claves entregadas por la autoridad de certificación CA-SSL.
- **Capa de Comunicación**. Hace efectiva la comunicación con el Administrador de Cuentas a través del protocolo SSL (*Secure Socket Layer* – Capa de Sockets Segura).

3.1.6. Interfaz al Banco

Este módulo permite realizar la interacción con el banco que ofrece a los usuarios las cuentas bancarias habilitadas para pagos móviles. Debe implementar los acuerdos de nivel de servicio y las condiciones de seguridad exigidas por el banco, así que en su mayoría depende de las características de esta entidad más que de las propias.

Por la dificultad que plantea realizar este tipo de negociaciones con el banco y dado que en esta tesis se realiza una propuesta académica implementada en un ambiente de prueba, el diseño de

esta interfaz simula muchas de las condiciones necesarias para establecer una relación entre la arquitectura propuesta y un Banco, pero no la totalidad.

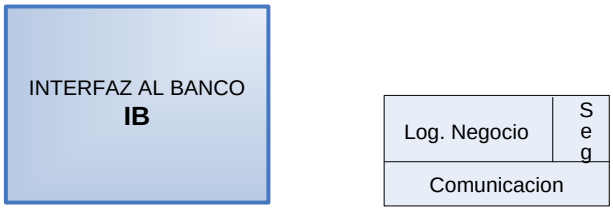


Figura 12. Interfaz al Banco

- **Capa de Lógica del Negocio**. Se encarga de recibir la información enviada por el Administrador de Cuentas, y adecuarla a los formatos manejados por el banco. También debe recibir la información enviada por el banco y transferirla al Administrador de Cuentas en el formato que previamente se haya establecido.
- **Capa de Seguridad.** Se encarga de verificar la identidad del Administrador de Cuentas y del banco a través de la autoridad de certificación definida. Toda la información intercambiada con el Administrador de Cuentas se debe cifrar de acuerdo a las claves dadas por dicha autoridad de certificación.
- **Capa de Comunicación**. Hace efectiva la comunicación con el Administrador de Cuentas a través de la implementación del protocolo de comunicación seguro SSL. También realiza la comunicación con el banco, típicamente utilizando protocolos propietarios.

3.1.7. Proveedor de Mensajes

Es el encargado de enviar mensajes al dispositivo móvil del usuario, a solicitud del Administrador de Cuentas. Los mensajes que se envían al usuario son mensajes de confirmación de realización de un servicio, ya sea con respecto a la cuenta o al pago. Este módulo también se encarga de solicitarle al Proveedor de Correo, el envío de la factura digital al usuario.

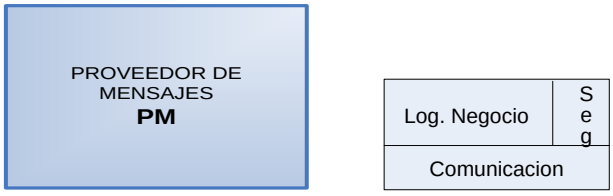


Figura 13. Proveedor de Mensajes

- **Capa de Lógica del Negocio**. Se encarga de todo el proceso de enviar, al dispositivo móvil del usuario, los mensajes que le han sido entregados por el Administrador de Cuentas. También se encarga del envío al Servidor de Correo de la factura digital generada por el Administrador de Cuentas, después de que ha sido firmada digitalmente.
- **Capa de Seguridad**. Se encarga de firmar digitalmente, a través de la autoridad de certificación CA-B, la factura digital, que será enviada por el servidor de correo a la cuenta de correo definida por el usuario en el momento de creación de la cuenta del servicio de facturación y pago.
- **Capa de Comunicación**. Se encarga de establecer una comunicación con el Administrador de Cuentas a través de la implementación del protocolo seguro de comunicación HTTPS. También

debe implementar los mecanismos para el envío de los mensajes de texto y la factura digital al dispositivo móvil del usuario, estableciendo para ello comunicación con un servidor de mensajería y un servidor de correo.

3.2. Descripción de la Arquitectura

Una arquitectura permite que diferentes partes trabajen en conjunto para formar un todo funcional, para lograr esto la descripción de la arquitectura debe ser tal que permita entender, construir y mantener el sistema que ella representa. Una arquitectura es una entidad compleja que no puede ser descrita de una única forma unidimensional, por ello, uno de los conceptos más importantes asociados con la documentación de las arquitecturas de software es el concepto de Vista [40].

Una vista se puede definir como una representación de un conjunto de elementos de un sistema y las relaciones entre ellos. Cada vista enfatiza ciertos aspectos del sistema mientras ignora otros con la finalidad de hacer manejable el problema. Nunca una sola vista documenta totalmente la arquitectura. La documentación y descripción total se logra con un completo conjunto de vistas y la información asociada a ellas [40].

Dentro de los estilos de vistas, aparece el estilo modular el cual, entre otros aspectos, es la base para el análisis de la arquitectura. Como mínimo, las vistas modulares permiten determinar cómo el código fuente de un sistema puede dividirse en partes separadas, cómo ve cada parte los servicios provistos por los otros módulos y cómo todas esas partes deben ser ensambladas. El tipo de modularización determina como los cambios de una parte afectan a las otras y determinará por tanto la habilidad del sistema para soportar modificaciones, portabilidad y re-utilización.

La descripción de la arquitectura de facturación y pago se basa en vistas modulares relacionadas con las fases del desarrollo del sistema, Requerimientos, Análisis, Diseño e Implementación. Los requerimientos ya han sido especificados en los apartados anteriores cuando se hizo la caracterización de la plataforma, y la implementación se reflejará en el desarrollo del piloto de prueba realizado para la validación de la plataforma.

La fase de análisis [41] está relacionada con la abstracción primaria (clases y objetos) y los mecanismos presentes en el dominio del problema. Se identifican las clases que permiten modelar el sistema y las relaciones entre ellas, esto se muestra en una vista lógica de la estructura de clases a este nivel, denominada vista de análisis.

En la fase de diseño [41] se expande el resultado de la fase de análisis a una solución técnica. Las clases se refinan para proveer la infraestructura técnica: interfaces de usuario, manejo de bases datos, comunicación con otros sistemas, entre otros. Las clases de la fase de análisis son embebidas en esta infraestructura haciendo posible cambios tanto en el dominio del problema (análisis) como en la infraestructura (diseño). El resultado de esta fase se muestra en una vista lógica denominada vista de diseño.

Las vistas de análisis y diseño se detallan en los siguientes apartados.

3.2.1. Vista de Análisis

3.2.1.1. Dispositivo Móvil

Dependiendo de la tecnología de contacto que se tenga en el dispositivo móvil (RFID o NFC) se tiene una vista de análisis diferente.

Móvil RFID

En la Figura 14 se muestra la vista de análisis del dispositivo móvil, cuando se le adiciona una etiqueta RFID, como tecnología de contacto, para acceder al servicio de facturación y pago.

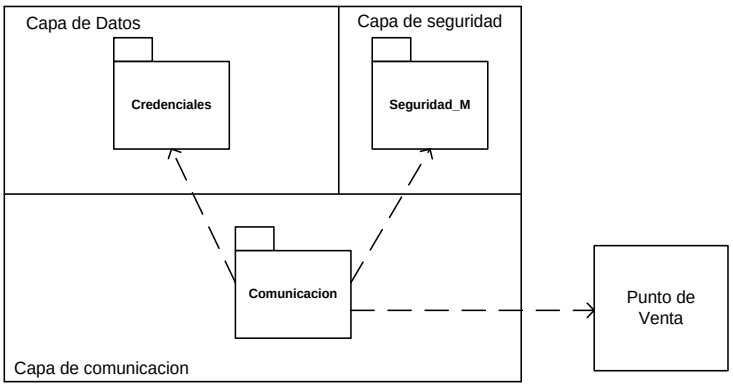


Figura 14. Diagrama de paquetes Móvil RFID

Debido a que la etiqueta RFID adicionada al dispositivo móvil es totalmente independiente del mismo, las funcionalidades de las capas de este módulo son provistas desde la misma etiqueta y no desde alguna aplicación desarrollada dentro del dispositivo.

Capa de Datos

- *Credenciales*: corresponde a los datos de usuario almacenados en la etiqueta RFID, estos son leídos por el lector ubicado en el Punto de Venta y permiten la validación del cliente del servicio de facturación y pago.

Capa de Seguridad

- *Seguridad_M:* contiene los certificados, llaves y demás herramientas proporcionan algoritmos de cifrado y procedimientos para la autenticación y autorización mutua, empleadas para brindar seguridad en la comunicación entre el lector y la etiqueta, los cuales son implementados por el fabricante de la etiqueta RFID.

Capa de Comunicación

- *Comunicación*: utiliza el protocolo de contacto cercano RFID empleado por la etiqueta para entablar una comunicación con el Lector.

Móvil NFC

En la Figura 15 se muestra la vista de análisis del dispositivo móvil, cuando utiliza como tecnología de contacto cercano a NFC.

Capa de Presentación

- *Interfaz_Usuario*: contiene las clases necesarias para crear la interfaz gráfica, desde la cual el cliente puede interactuar con la aplicación de pago instalada en su dispositivo móvil.

Capa de Lógica del Negocio

- *Lógica*: corresponde a una aplicación validada por una autoridad de certificación aceptada por el móvil, que le permite al cliente activar el pago.

Capa de Acceso Datos

- *Interfaz_ElementoSeguro*: se refiere a una aplicación firmada por una autoridad de certificación confiable para el equipo, la cual se constituye en la interfaz entre la *Lógica* y los datos almacenados en el elemento seguro NFC del teléfono móvil.

Capa de Seguridad

- *Seguridad*: contiene los certificados digitales tanto del paquete *Lógica* y de *Interfaz_ElementoSeguro* que permiten catalogarlos como confiables.

Capa de Datos

- *Credenciales*: corresponde a los datos del usuario y de la cuenta del servicio almacenados en el elemento seguro NFC del teléfono, los cuales son leídos por el lector ubicado en el Punto de Venta. Estas credenciales permiten la autenticación del cliente del servicio de facturación y pago y lo autorizan para utilizar el servicio.

Capa de Comunicación

- *Comunicación*: contiene las API que implementan el protocolo NFC utilizado por el teléfono móvil para comunicarse con el Lector ubicado en el Punto de Venta o en el Punto de Creación de la Cuenta. El protocolo NFC garantiza que esta comunicación es segura ya que incluye mecanismos de autenticación segura y anticolisión para evitar la escucha del canal de comunicación, además usa cifrado AES y triple-DES con lo que la seguridad se equipara a las ofrecidas por las tarjetas inteligentes bancarias.

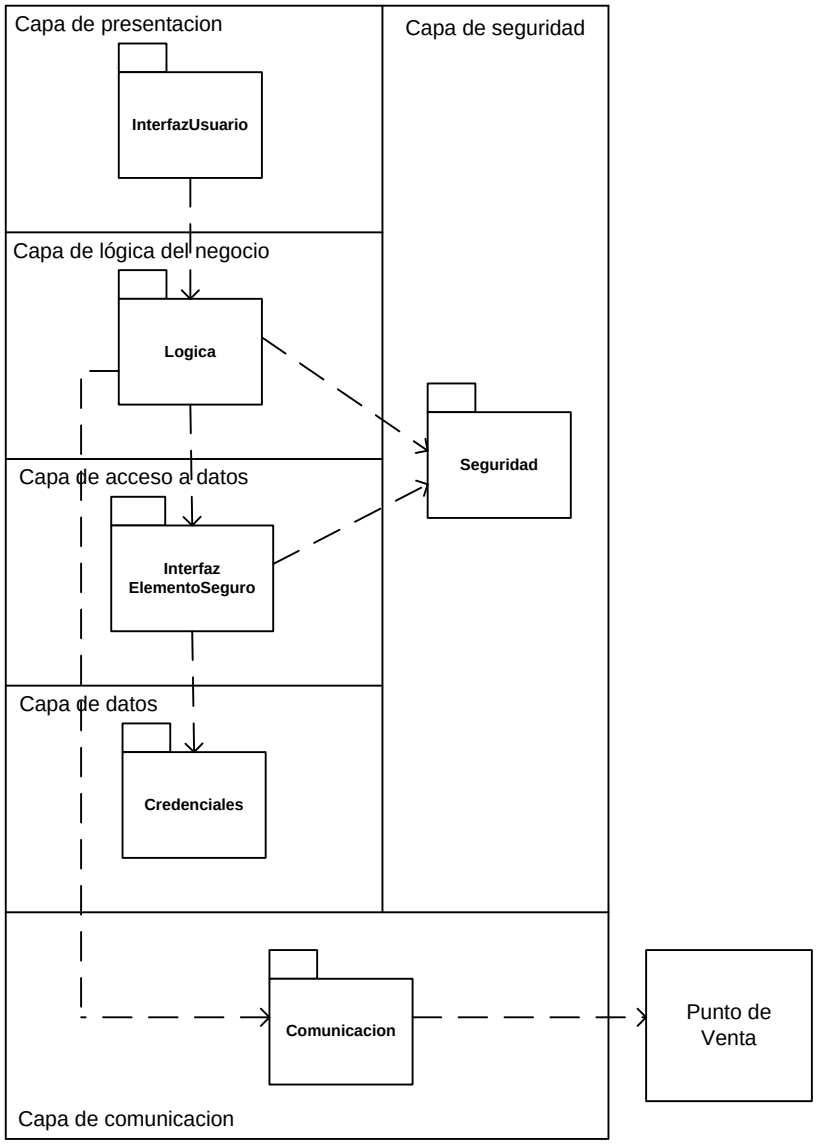


Figura 15. Diagrama de Paquetes Móvil NFC

3.2.1.2. Punto de Venta

La Figura 16 muestra la vista de análisis del módulo Punto de Venta.

Capa de Presentación

- *InterfazVenta*: representa a las clases de la interfaz de escritorio provista para el registro de los almacenes en la plataforma de facturación y pago, y que el vendedor asociado a cada almacén esté al tanto del resultado de las transacciones.

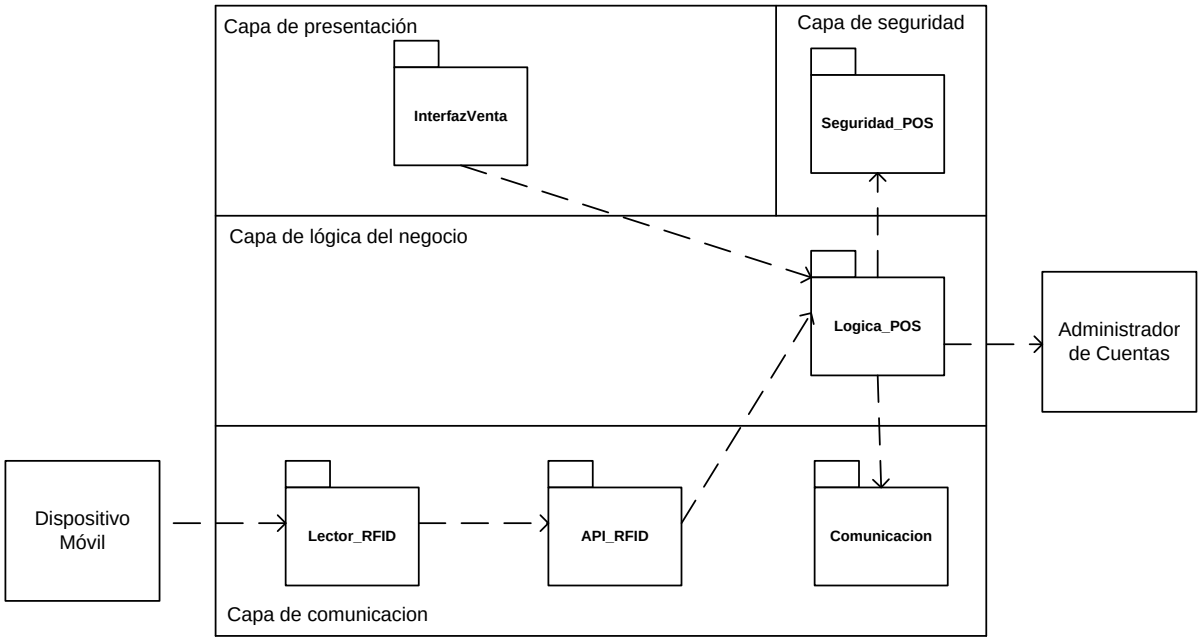


Figura 16. Vista de Análisis Punto de Venta

Capa de Lógica de Negocio

- *Logica_POS*: corresponde a las clases, paquetes y demás recursos que permiten coordinar el acceso al Administrador de Cuentas y a las credenciales almacenadas en el elemento seguro del dispositivo móvil (etiqueta RFID/NFC).

Capa de Seguridad

- *Seguridad_POS*: integra a los archivos y herramientas que permiten crear una comunicación segura, garantizando la autenticación y la confidencialidad de la información que se transfiere entre este módulo y el Administrador de Cuentas.

Capa de Comunicación

- *Comunicación*: se refiere a las clases que permiten la implementación del protocolo de comunicación segura con el Administrador de Cuentas. Este protocolo maneja técnicas de cifrado para garantizar la confidencialidad de la información, además garantiza la autenticidad de las partes, para lo cual se basa en la autoridad de certificación CA-SSL.
- *Lector_RFID*: corresponde al dispositivo que permite leer la información almacenada en el elemento seguro del dispositivo móvil.
- *API_RFID*: representa las librerías y herramientas que permiten la conexión de la aplicación desarrollada con el lector de etiquetas.

3.2.1.3. Punto de Creación de la Cuenta

Los paquetes de este módulo son los mismos que los del Punto de Venta, solamente cambia la funcionalidad del paquete Lógica. Las solicitudes hechas al Administrador de Cuentas por este módulo están relacionadas con la administración de las cuentas: crearlas, modificarlas o eliminarlas; para esto debe enviar los datos del cliente al Administrador de Cuentas y este a su vez le envía el resultado de las acciones solicitadas.

3.2.1.4. Administrador de Cuenta

En la Figura 17 se muestra la vista de análisis del módulo Administrador de Cuentas de la arquitectura. A continuación se detalla la funcionalidad de cada uno de las capas que lo conforman.

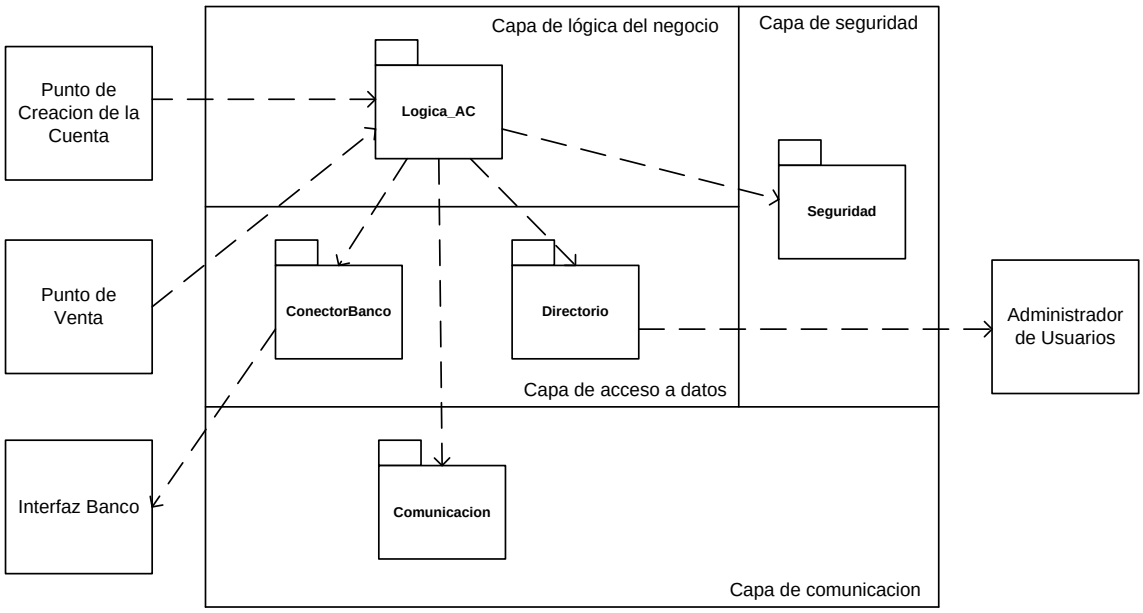


Figura 17. Vista de Análisis Administrador de Cuentas

Capa de Lógica de Negocio

- *Lógica_AC*: contiene los paquetes, librerías y herramientas que permiten la ejecución de las funciones para atender las solicitudes del POS y del PCC. Estas solicitudes pueden ser de verificación de pago, creación, eliminación y modificación de cuenta. Además este módulo contiene las funcionalidades adecuadas para notificar al usuario o vendedor del resultado de la acción ejecutada.

Capa de Acceso Datos

- *Directorio*: integra el API y los paquetes que permiten el acceso a las bases de datos de los usuarios, las cuales se encuentran en el módulo Administrador de Usuarios.
- *ConectorBanco*: son las clases y recursos que permiten el acceso al Banco.

Capa de Seguridad

- *Seguridad*: herramientas que permiten una comunicación segura, mediante el cifrado de la información, con los módulos Punto de Venta, Punto de Creación de Cuentas y Administrador de Usuarios.

Capa de Comunicación

- *Comunicación*: representa el uso de los protocolos que permiten la comunicación con los módulos Punto de Venta y Punto de Creación de la Cuenta.

3.2.1.5. Administrador de Usuarios

La vista de análisis del módulo Administrador de Usuario se muestra en la Figura 18.

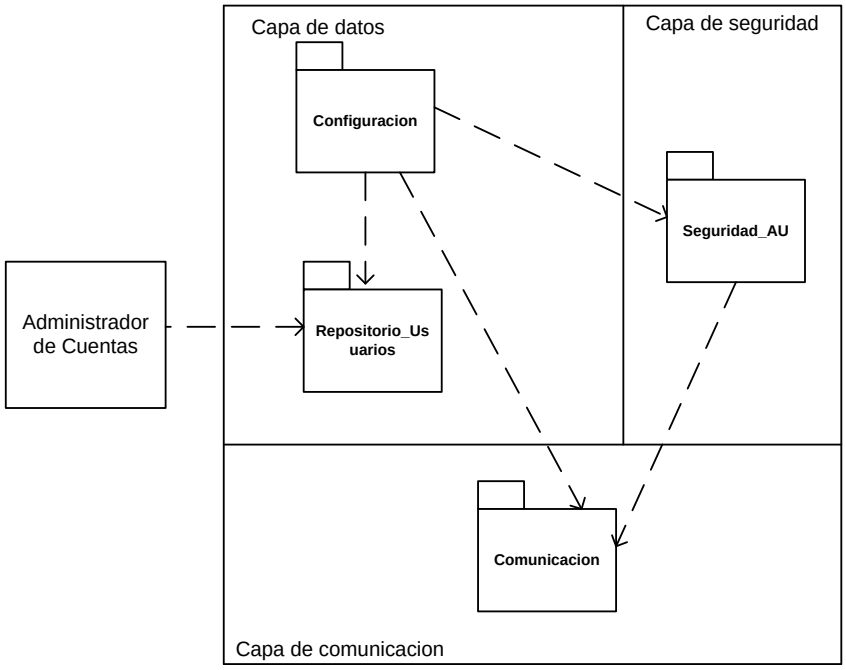


Figura 18. Vista de Análisis Administrador de Usuarios

Capa de Seguridad

- *Seguridad_AU*: está conformado por los archivos y herramientas que permiten crear una comunicación segura con el Administrador de Usuarios

Capa de Datos

- *Configuración*: contiene los archivos de configuración del repositorio donde se almacenan los datos del usuario. En este paquete se definen las características y propiedades del servicio de repositorio, como el administrador y su clave, el tipo de base de datos y el archivo donde se almacenarán todos los datos del directorio.

- *Repositorio_Usuarios*: contiene el repositorio donde se almacena la información de los usuarios.

Capa de Comunicación

- *Comunicación*: está conformado por las funciones que implementan el protocolo seguro LDAPS que permite que el módulo Administrador de Cuentas tenga acceso al repositorio donde están almacenados los datos de los usuarios.

3.2.1.6. Proveedor de Mensajes

En la Figura 19 se muestra la vista de análisis del módulo Proveedor de mensajes.

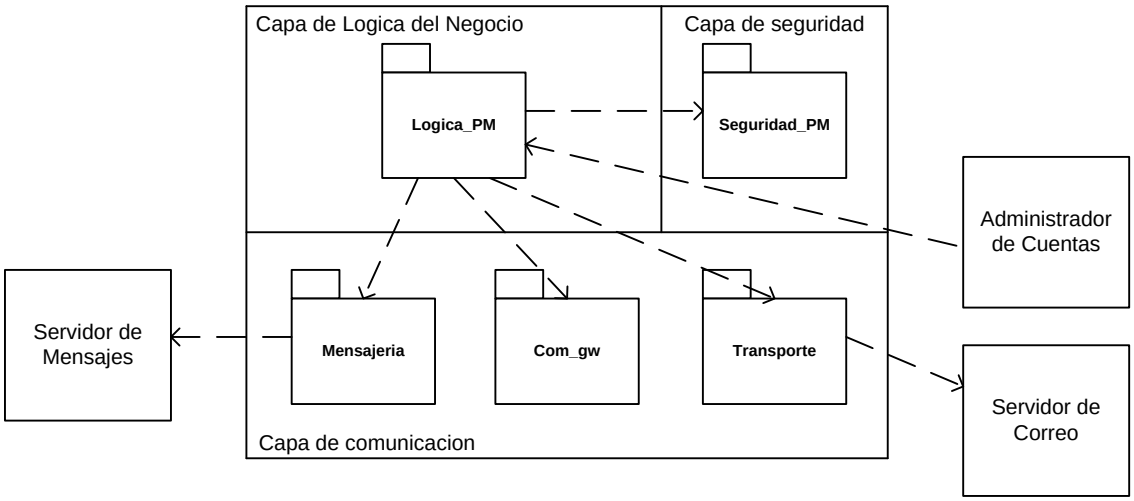


Figura 19. Vista de Análisis Proveedor de Mensajes

Capa de Lógica de Negocio

- *Lógica_PM*: son las clases encargadas de coordinar el envío de mensajes y cada una de las operaciones requeridas para dicho propósito, como recibir los datos del usuario y enviarlos al móvil que actúa como pasarela entre la red cableada y la red celular. Además *c*ontiene las clases mediante las cuales se establece una sesión con un servidor de correo, en este paquete además se configuran los datos del destinatario, el remitente y el mensaje.

Capa de Seguridad

- *Seguridad_PM*: se encarga de firmar digitalmente la factura digital enviada por el módulo Administrador de Cuentas, esta operación la realiza por medio de la autoridad de certificación CA_B. Además, contiene los recursos mediante los cuales se brinda seguridad a través de mecanismos de cifrado en la sesión establecida con el Servidor de Correo.

Capa de Comunicación

- *Mensajería*: contiene las librerías y todas las herramientas necesarias para hacer efectivo el envío de mensajes de texto.

- *Com_gw*: contiene las API que permiten la comunicación con el teléfono móvil, que desempeña el papel de *gateway* de mensajería corta.
- *Transporte*: Contiene las clases que permiten la implementación del protocolo empleado para el envío del correo (SMTP).

3.2.2. Vista de Diseño de la Arquitectura

A continuación se presenta las decisiones de diseño adoptadas para la arquitectura y la descripción de la vista de diseño para cada uno de los módulos que la conforman.

3.2.2.1. Dispositivo Móvil

Decisiones de Diseño

Cuando la tecnología que se utiliza en el dispositivo móvil es RFID, se debe seleccionar la etiqueta respectiva, la cual, de acuerdo a sus características y al fabricante, define particularidades de diseño de este módulo de la arquitectura de facturación y pago.

Los dos tipos más comunes de etiquetas RFID son activas y pasivas. Las etiquetas RFID activas tienen su propia fuente de energía, alcanzan mayor distancia de comunicación, usualmente tienen más capacidad de almacenamiento y tienden a ser más costosas que las pasivas. Las etiquetas pasivas RFID están disponibles sin y con chips, y no tienen una fuente de energía propia por lo cual requieren de una externa para operar [42].

Existen varias bandas dentro de las cuales puede operar la tecnología RFID pasiva, obteniendo la siguiente clasificación: RFID pasiva en LF (*Low Frequency*), RFID pasiva en HF (*High Frecuency*) y RFID pasiva en UHF (*Ultra High Frecuency*) [43].

Las etiquetas RFID LF utilizan las frecuencias de 125 y 134,2 Khz, son bastante costosas y no soportan lectura simultánea de etiquetas.

Las etiquetas RFID UHF trabajan en el rango de frecuencias entre 300MHz y 3GHz en el espectro de radio, permiten mayores distancias y antenas más pequeñas, son etiquetas más económicas pero carecen de regulación y estándares globales [43]. Los costos y la falta de regulación hacen que estas etiquetas sean poco viables para su uso dentro de la arquitectura propuesta.

Por otro lado, las etiquetas RFID HF operan a 13.56 MHz la cual es una frecuencia aceptada globalmente. Las antenas de las etiquetas HF son pequeñas, lo suficiente para producirlas por medio de una impresión en un sustrato, usando tinta conductiva para luego ser fijada en un chip, permiten alta tasa de transmisión de datos, las etiquetas son más económicas y con mayor capacidad de memoria, el rango de lectura es menor a un metro, la frecuencia es usada y reconocida globalmente (sin restricciones), existen estándares Globales: ISO 15693, 14443, 18000-3 [43]. Dadas todas estas características dentro de la arquitectura se utiliza una etiqueta pasiva HF.

La etiqueta seleccionada es la iClass Tag 206x del fabricante HID Corp. La tecnología iCLASS® [44] está diseñada para hacer el control de acceso más seguro y basado en estándares, características importantes dentro de la arquitectura:

- Toda la transmisión de datos por radiofrecuencia entre la tarjeta y el lector se codifica utilizando un algoritmo seguro y utilizando técnicas de cifrado estándares de la industria, iCLASS reduce el riesgo de que la seguridad de la información esté en peligro.
- Para más seguridad aún, los datos de la tarjeta también pueden protegerse con cifrado DES o triple DES.
- Contiene múltiples áreas de aplicación, separadas para garantizar seguridad, que se encuentran protegidas por llaves diversificadas de lectura/escritura, de 64-bit, que permiten implementar aplicaciones complejas y facilitan la ampliación en el futuro.
- La comunicación entre la etiqueta y el lector cumple con los estándares 14443B lectura/escritura (16k solamente) y 15693 lectura/escritura.

Vista de Diseño

Teniendo en cuenta los aspectos mencionados, en la Figura 20 se muestra el diagrama de paquetes de diseño del componente Móvil RFID de la arquitectura.

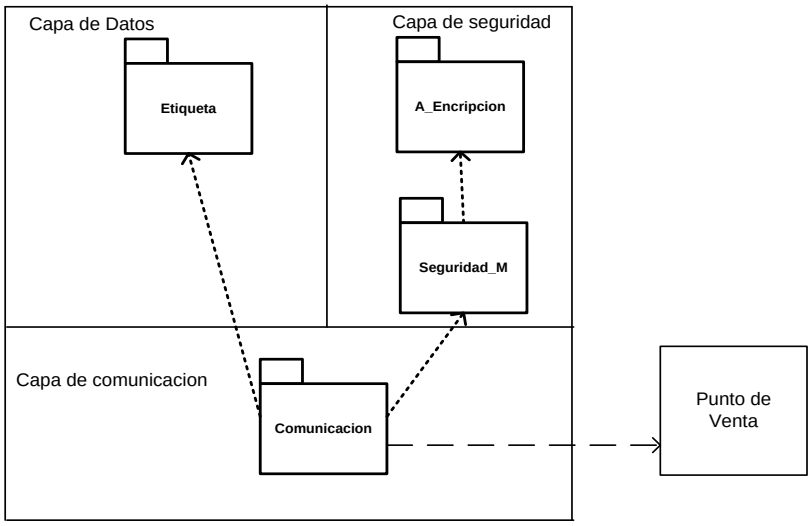


Figura 20. Diagrama de Paquetes de Diseño Dispositivo Móvil RFID

Capa de Datos

- *Etiqueta*: los datos de usuario (credenciales) se almacenan en una etiqueta RFID. Esta etiqueta para el caso de estudio fue una iCLASS Tag 206X que tiene capacidad de 2KBytes y según la referencia empleada: 2061 o 2062 tiene 2 o 16 áreas de aplicación definidas por el fabricante [44].

Capa de Seguridad

- *Seguridad_M:* se encarga de cifrar la información a transmitir al lector, a través del uso del algoritmo seguro predefinido por el fabricante de las etiquetas. También implementa la autenticación mutua que debe existir entre el lector y la etiqueta.
- *A_Cifrado:* se refiere a la librería que implementa el algoritmo usado para cifrar los datos que se almacenan en la etiqueta. Para las etiquetas seleccionadas el mejor algoritmo es 3DES.

Capa de Comunicación

- *Comunicación*: se refiere al estándar ISO 14443B que regula la comunicación entre el lector y la etiqueta RFID, ya que define el protocolo T = CL para el intercambio de las APDU (*Application Protocol Data Unit* – Unidad de Datos del Protocolo de Aplicación) entre los dispositivos mencionados [46].

3.2.2.2. Punto de Venta

Decisiones de Diseño

El módulo Punto de Venta contiene una interfaz agradable y de fácil manejo para el vendedor. Esta interfaz está basada en formularios para permitir el registro del punto de venta ante el servicio, y además que el vendedor vea el resultado de la operación de registro y del proceso de pago. El desarrollo de este módulo se hace en Java y para los formularios se usa el API Forms de Swing [46] los cuales son flexibles e independientes de la plataforma que lo hacen adecuado para la implementación de las interfaces y le dan la característica de interoperabilidad a la arquitectura.

El lector usado en este módulo se define de acuerdo a las etiquetas RFID seleccionadas. La comunicación entre etiqueta y lector se realiza a través del protocolo definido por el fabricante. Para la comunicación de la aplicación implementada en el Punto de Venta y el lector se utiliza el HID *Serial Protocol* [47]. Para el acceso a la información de las etiquetas RFID se utiliza JNI (*Java Native Interface*) [48], framework de programación que permite que un programa escrito en Java ejecutado en la máquina virtual java (JVM) pueda interactuar con programas escritos en otros lenguajes como C, C++ y ensamblador. Esto se requiere ya que el software que se encuentra en el lector no es Java.

La comunicación con el módulo Administrador de Cuentas se realiza a través de un cliente de Servicio Web, ya que ese módulo esta implementado en esta tecnología, como se explica más adelante. La seguridad en la comunicación entre este módulo y el Punto de Venta se implementa a través del protocolo WS-Security (Seguridad en Servicios Web) [49], el cual suministra un medio para aplicar seguridad a los Servicios Web y que contiene especificaciones sobre cómo debe garantizarse la integridad y seguridad en mensajería de Servicios Web. El protocolo WSS incluye detalles en el uso de SAML (*Security Assertion Markup Language*) [50] y Kerberos, y formatos de certificado tales como X.509.

WS-Security incorpora características de seguridad en el encabezado de un mensaje SOAP, trabajando en la capa aplicación. Así asegura seguridad extremo a extremo [49], a diferencia de otros mecanismos como TLS (*Transport Layer Security* – Seguridad en la Capa de Transporte) que solo garantiza la seguridad punto a punto. Este aspecto es importante para la arquitectura ya que independiente de la infraestructura de red que permita la comunicación entre el Punto de Venta y el Administrador de Cuentas, WS-Security permite que la información viaje segura durante todo el trayecto.

Vista de Diseño

Teniendo en cuenta las especificaciones anteriores, en la Figura 21 se ilustra el diagrama de paquetes de diseño del Punto de Venta.

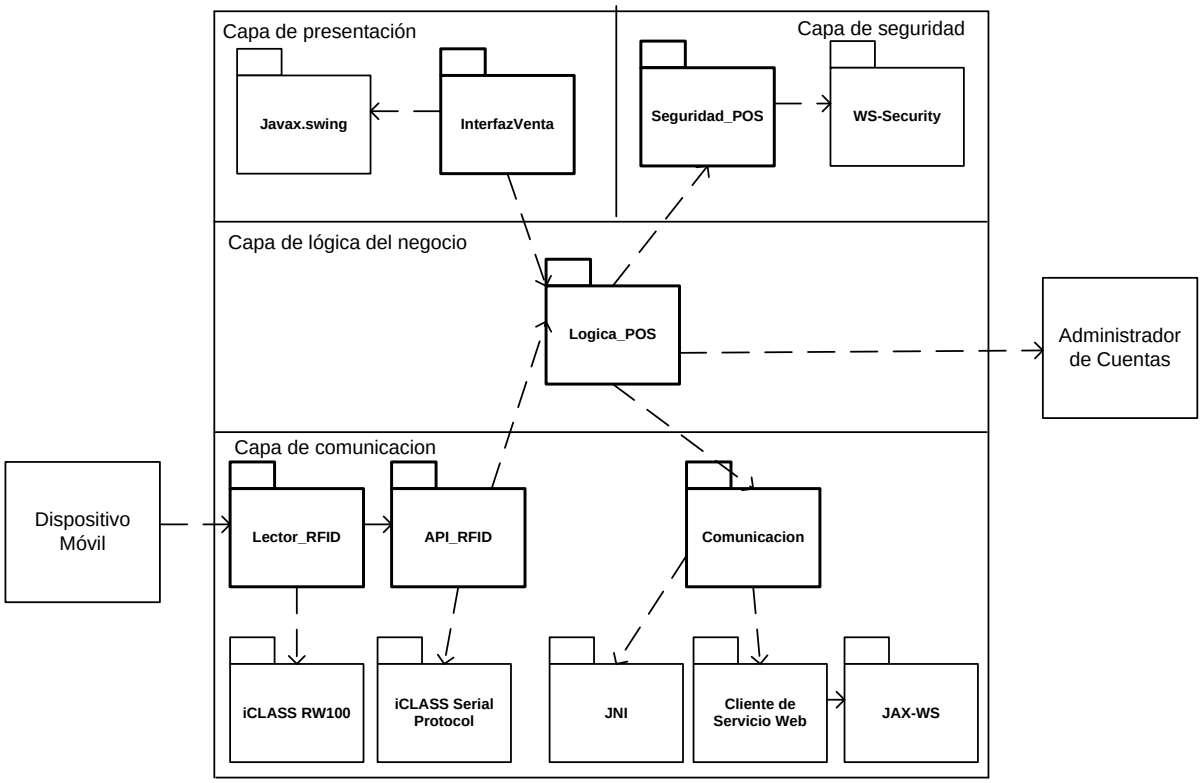


Figura 21. Diagrama de Paquetes de Diseño Punto de Venta

Capa de Presentación

- *InterfazVenta*: contiene las clases que permiten visualizar de forma agradable para el vendedor, las interacciones entre el POS y el AC. Utiliza *Forms* de *Java Swing* para realizar el registro del Punto de Venta ante el servicio y ver los mensajes resultantes de las transacciones realizadas.

Capa de Seguridad

- *Seguridad_POS*: representa la implementación de WS-Security, que impide a usuarios no autorizados acceder al AC, mediante esquemas como autenticación de nombre de usuario con llave simétrica, SSL, autorización SAML, entre otros.

Capa de Lógica de Negocio

- *Logica_POS*: se refiere a toda la lógica detrás del Nivel de Presentación, encargada de determinar que interfaz de comunicación debe usarse en una determinada operación (puerto USB, Cliente de Servicio Web implementado), y también responsable de validar que las

credenciales de seguridad enviadas tengan el formato adecuado, luego de ser leídas en las etiquetas.

Capa de Comunicación:

- *Comunicación*: la comunicación del Punto de Venta se realiza básicamente usando JNI (Java Native Interface)[48], que permite acceder al lector de RFID, recibir y enviar información proveniente de etiquetas. Y un Cliente de Servicio Web que es usado cuando se necesita usar funcionalidad del AC y se soporta en JAX-WS (XML-Based Web Services)[51].
- *API_RFID*: representa el Protocolo Serial de Comunicaciones de HID Corp, que es propietario, y permite una comunicación efectiva con el lector, ya que sin este aunque se disponga del acceso a un puerto USB, no se sabría que formato tienen las instrucciones aceptadas.
- *Lector_RFID*: se refiere al dispositivo (lector) necesario para leer medios de almacenamiento NFC y/o RFID.

3.2.2.3. Punto de Creación de Cuentas

Decisiones de Diseño

Las decisiones de diseño tomadas para este módulo son las mismas que para el Punto de Venta, por tanto los paquetes son los mismos.

Vista de Diseño

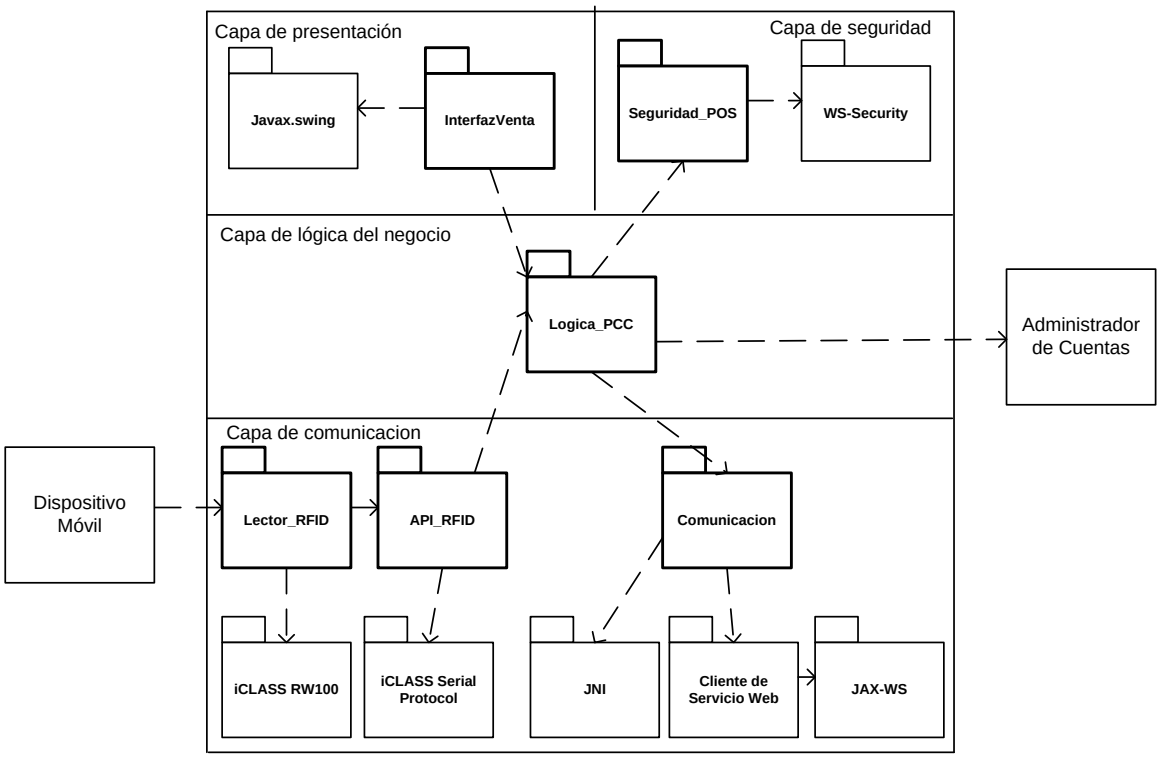


Figura 22. Diagrama de Paquetes de Diseño Punto de Creación de la Cuenta

La diferencia con el módulo Punto de Venta radica en la funcionalidad del paquete de la capa de lógica del negocio, cuyo nombre es Logica_PCC, como se muestra en la Figura 22.

Capa de Lógica de Negocio

- *Logica_PCC*: se refiere a toda la lógica detrás del Nivel de Presentación, encargada de determinar que interfaz de comunicación debe usarse en una determinada operación (puerto USB, Cliente de Servicio Web), y también responsable de recibir la clave generada para un usuario que se encuentra en el proceso de crear una cuenta de servicio y comprobar que sus credenciales fueron grabadas correctamente en la etiqueta antes de entregarla.

3.2.2.4. Administrador de Cuentas

Decisiones de Diseño

El módulo Administrador de Cuentas tiene como función principal controlar y coordinar todo los procesos que se deben llevar a cabo para realizar las operaciones de pago y facturación, para ello debe establecer comunicación con la mayoría de módulos de la arquitectura.

La comunicación con el Administrador de Usuarios, en donde se encuentra el servidor de directorio que almacena toda la información de los usuarios y sus cuentas, se realiza a través de JNDI (*Java Naming and Directory Interface*) .

JNDI además de trabajar con servicios de nombrado también se relaciona con servicios de directorio, los cuales son una extensión natural de los servicios de nombrado. El servicio de directorio permite asociar atributos a los objetos y buscar los objetos basados en dichos atributos.

Asociado a JNDI API, aparece JNDI SPI (*Service Provider Interface*) que permite trabajar con diferentes clases de proveedores de servicios de nombrado y de directorio. El uso de esta interfaz le brinda flexibilidad a la arquitectura, ya que si se requiere trabajar con un servicio de directorio diferente a LDAP, que es el utilizado en el módulo de Administrador de Usuarios, dicha transición se podría hacer de manera transparente para los demás módulos.

El Administrador de Cuentas está implementado como un Servicio Web, lo cual le da la característica de interoperabilidad a la arquitectura. Los Servicios Web son altamente interoperables ya que están basados en estándares abiertos.

Los servicios web también permiten una gran flexibilidad debido a que aportan gran independencia entre la aplicación que usa el servicio Web y el propio servicio, en este caso entre los módulos Punto de Venta y Punto de Creación de la Cuenta y el Administrador de Cuentas. De esta forma, los cambios a lo largo del tiempo en uno no deben afectar al otro.

La comunicación con los módulos Punto de Venta y Punto de Creación de la Cuenta se basa en JAX-WS (*Java API for XML Web Services*) [51] que es una API de Java para la creación y comunicación de Servicios Web. JAX-WS se desarrolla en la modalidad de código abierto y hace parte del proyecto *GlassFish* [52] que es un servidor de aplicaciones de Java EE (*Enterprise Edition*) de código abierto.

Por otro lado, la comunicación del Administrador de Cuentas con la Interfaz al Banco dependerá de las características impuestas por este. Para el caso de la arquitectura esta interfaz se asume simplemente como una base de datos (por simplicidad de implementación MySQL), en la cual se encuentra la información de la cuenta financiera del cliente, y a la cual se accede a través del patrón DAO (*Data Access Object*) [53] que es un componente de software que suministra una interfaz común entre la aplicación y uno o más dispositivos de almacenamiento de datos, tales como una base de datos o un archivo y que también se puede implementar de manera fácil.

Para asegurar la comunicación con los módulos con los cuales el módulo Administrador de Cuentas intercambia información sensible se manejaron dos esquemas de seguridad: protocolo de seguridad SSL (*Secure Socket Layer*) y WS-Security.

La comunicación con el modulo Administrador de Usuarios se realiza a través del uso del protocolo de seguridad SSL [54]. SSL proporciona autenticación y privacidad de la información entre extremos mediante el uso de criptografía. La autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten que la comunicación entre el Administrador de Cuentas y el Administrador de Usuarios se realice de una forma diseñada para prevenir escuchas (*eavesdropping*), la falsificación de la identidad del remitente (*phishing*) y mantener la integridad del mensaje.

SSL implica una serie de fases básicas: Negociar entre las partes el algoritmo que se usará en la comunicación, el intercambio de claves públicas y autenticación basada en certificados digitales y por último el cifrado del tráfico basado en técnicas simétricas, para lo cual se usan los servicios de la autoridad de certificación CA-SSL que es la encargada de la generación de las claves.

El otro esquema de seguridad se implementó para asegurar la información entre el Administrador de Cuentas y los módulos Punto de Venta y Punto de Creación de la Cuenta, y está basado en WS-Security que, como se explicó, garantiza la seguridad en la comunicación en Servicios Web.

Para efectos de implementación y ya que no fue posible adquirir los certificados a través de alguna entidad certificadora real, debido a los costos de los mismos, se realizó la generación de los certificados digitales a través del software X-CA [55], el cual corresponde a una interfaz de usuario gráfica para openSSL, útil para la generación de claves públicas RSA, certificados, requerimientos de firmas y listas de revocación.

Vista de Diseño

En la Figura 23 se detallan los paquetes de diseño que implementan los conceptos mencionados.

Capa de Lógica de Negocio

- *Lógica_AC*: se refiere a las funciones de control y lógica involucradas en las comunicaciones realizadas por el Servicio Web, agrupadas de la siguiente manera:
- *AC_Control*: se encarga de definir una respuesta adecuada para cada solicitud, coordinar las operaciones de pago como accesos a cuenta y transacciones con el banco, además de solicitar el envío de mensajes SMS de notificación y de la factura digital.

- *AC_Logic*: se encarga de generar las facturas digitales en formato PDF, definir el contenido y tema de los correos electrónicos, y establecer el contenido de los mensajes de texto. Además, incluye un *Bean* de comunicación con la base de datos que simula al banco.

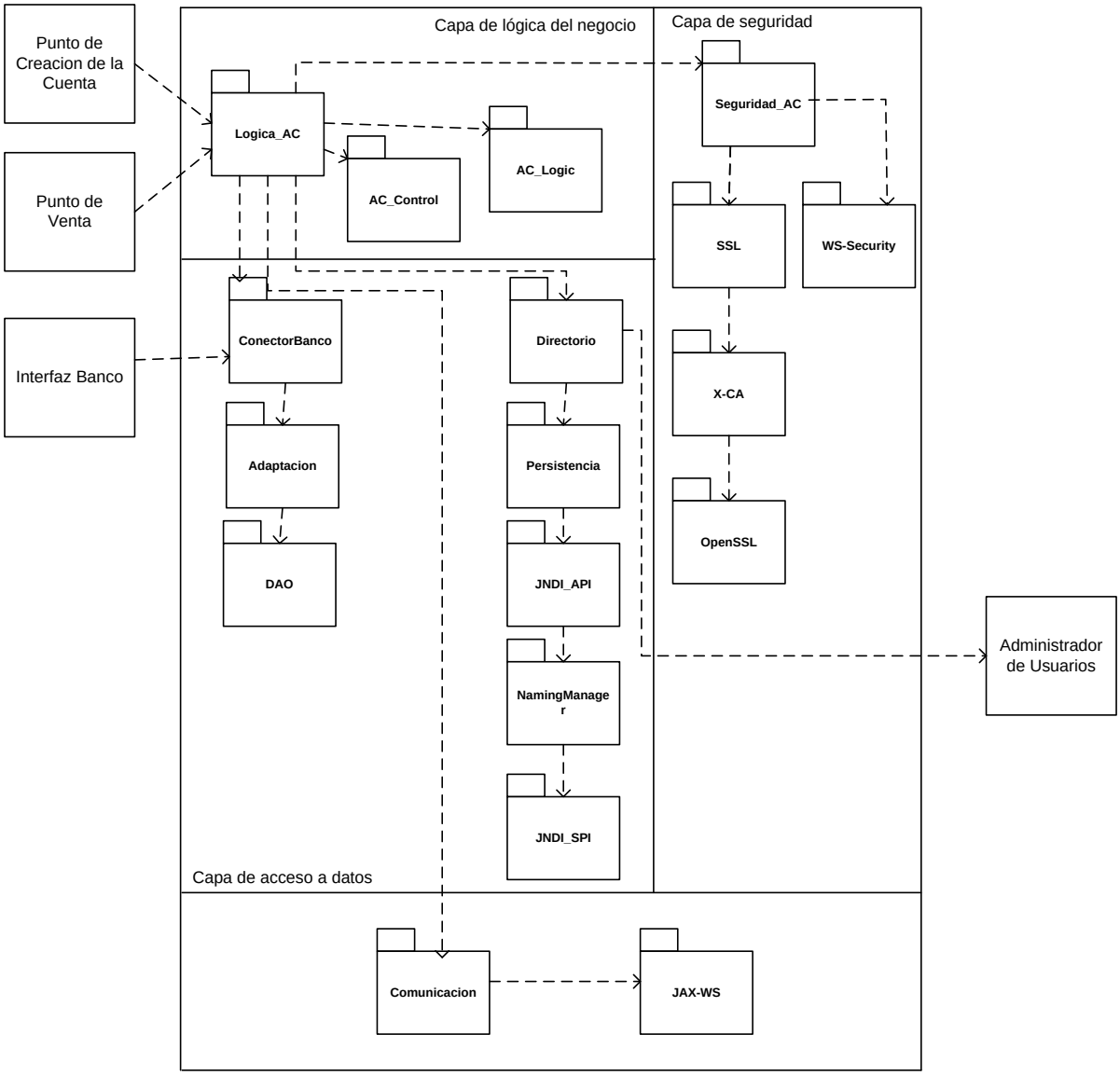


Figura 23. Paquetes de Diseño Administrador de Cuentas

Capa de Acceso a Datos

- *ConectorBanco:* se refiere a la conexión con la simulación del Banco que se basó en una base de datos de MySQL. Es un bloque de adaptación a las interfaces de comunicación que define el Banco, se accede a la información de las cuentas bancarias convencionales y limitadas empleando el patrón DAO.
- *Directorio*: representa todas las clases y paquetes involucrados en la comunicación cifrada con el servidor de directorio LDAP, que se han dividido de la siguiente manera:

- *Persistencia*: incluye las clases utilizadas al interior de LDAP, así como las clases necesarias para recuperar la información almacenada en un formato que pueda ser reconocido y manejado adecuadamente por el Servicio Web encargado de controlar todo el proceso de pago.
- *JNDI_API*: representa al paquete y clases que implementan el API JNDI y permiten acceder a sus capas subyacentes como son el *Naming_Manager* y JNDI_SPI, para finalmente establecer comunicación mediante el protocolo LDAPS (LDAP over SSL) con el Administrador de Usuarios.
- *Naming_Manager*: permite acceder a un servidor físico, en este caso un servidor corriendo el servicio de directorio LDAP. *Naming_Manager* permite independizar la implementación de acceso a directorio del servidor físico, de forma tal que este puede ser cambiado sin necesidad de efectuar cambios sobre el código de la aplicación.
- *JNDI_SPI*: permite conectarse de forma transparente con servicios de nombres y directorio, como DNS y LDAP, en este caso es con un directorio LDAP, pero si se necesitara cambiar por un servicio diferente este paquete facilitaría la transición.

Capa de Seguridad

- *Segurida_AC:* se refiere a las herramientas que necesita el Administrador de Cuentas para establecer comunicaciones cifradas con otros módulos definidos en la arquitectura. Estas herramientas se han organizado de la siguiente forma:
- *SSL*: para establecer comunicaciones mediante SSL es necesario la compra o generación de certificados digitales, que deben ser puestos en una ruta accesible por el Servicio Web, en este paquete se configura el acceso a los certificados digitales que permiten establecer conexiones TLS/SSL con el Administrador de Usuarios.
- *X-CA*: para facilitar la generación de certificados digitales se usó X-CA con el cual se creó una entidad certificadora propia.
- *OpenSSL:* se refiere a un paquete de herramientas que suministran funciones relacionadas con el cifrado de los datos. OpenSSL [56] también permite crear certificados digitales empleados para establecer comunicación mediante LDAPS.
- *WS-Security*: le permite al Administrador de Cuentas establecer conversaciones cifradas no basadas en SSL con el POS y con PCC, con la ventaja de garantizar seguridad extremo a extremo al contrario de SSL que establece relaciones de confianza en tramos de la comunicación.

Capa de Comunicación

- *Comunicación:* se basa en JAX-WS que es una especificación de comunicaciones para Servicios Web.

3.2.2.5. Administrador de Usuarios

Decisiones de Diseño

Este módulo está basado en un servicio de nombrado, cuyo propósito es asociar nombres con objetos y brindar una manera de acceder a dichos objetos basados en sus nombres. Los objetos en un sistema de nombrado pueden variar desde archivos en un sistema de archivos, nombres en

un sistema de nombres de dominio, componentes EJB (*Enterprise Java Beans*) en un servidor de aplicaciones, y perfiles de usuario en un directorio LDAP.

El almacenamiento de la información de los usuarios y sus cuentas y el acceso a dicha información se basa en LDAP [57]. LDAP es un protocolo del nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas. Habitualmente, almacena la información de *login* (usuario y contraseña) y es utilizado para autenticarse, característica que es usada dentro de la arquitectura, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, entre otros).

LDAP presenta las siguientes ventajas frente a una base de datos relacional y que constituyen las razones por las cuales fue seleccionado para la arquitectura:

- LDAP está diseñado para permitir lectura de datos muy rápida, no así la escritura. Ello lo convierte en solución idónea para almacenar información acerca de usuarios, la cual por norma general es mucho más consultada que modificada.
- LDAP propone una estructura jerarquizada de información frente a la organización relacional de una base de datos.
- LDAP no soporta complejos mecanismos de actualización o consulta. Las aplicaciones acceden al servicio de directorio LDAP de manera sencilla y eficiente.

La base de datos en la cual se almacenan los datos está basada en la tecnología Oracle Berkeley [58], que es un motor para bases de datos embebidas de alto rendimiento, el cual corre directamente en la aplicación que lo usa, por lo cual no requiere un servidor de bases de datos adicional, y no necesita administración, además de contar con características como acceso concurrente (cantidad de usuarios al mismo tiempo), transacciones (operaciones que se realizan completamente o no se realizan) y replicación, para ofrecer alta disponibilidad y tolerancia a fallos.

El Administrador de Usuarios establece una comunicación segura con el módulo Administrador de Cuentas a través del protocolo LDAPS, el cual es la implementación del protocolo LDAP sobre SSL.

Vista de Diseño

En la Figura 24 se muestran los paquetes de diseño que conforman este módulo.

Capa de Datos

- *Configuración:* la configuración del Servidor de Directorio se basa en el archivo de configuración *slapd.conf*, en el cual se especifican los esquemas de directorio necesarios, se definen listas de control de acceso para definir los privilegios de los usuarios, se especifica el nodo principal del árbol y las credenciales del usuario administrador, además de la ruta donde se guarda el directorio (una base de datos tipo Oracle Berkeley [58]).
- *Repositorio_Usuarios*: se refiere a la base de datos en la que el servidor de directorio guarda la información de los usuarios

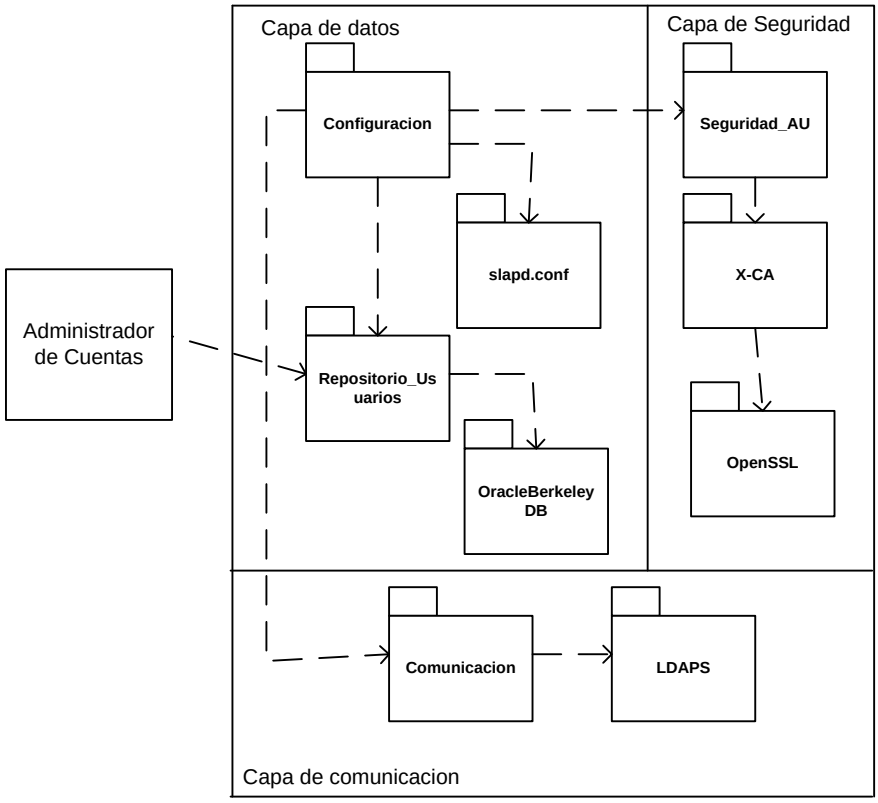


Figura 24. Paquetes de Diseño Administrador de Usuarios

Capa de Seguridad

- *Seguridad_AU:* es idéntico al paquete *Seguridad_AC,* a excepción de WS-Security. Ya que únicamente establece comunicaciones cifradas sobre SSL.

Capa de Comunicación:

- *Comunicación*: se refiere a la comunicación sobre SSL que proporciona el protocolo LDAPS.
- *LDAPS*: permite llevar a cabo la comunicación LDAP en un túnel SSL, empleando certificados digitales, esta comunicación se realiza por el puerto 636.

3.2.2.6. Proveedor de Mensajes

Decisiones de Diseño

El proveedor de Mensajes se encarga del envío de los mensajes de texto hacia el dispositivo móvil del usuario. Para poder tener acceso a la red celular, para el envío de los mensajes, se debe contar con un dispositivo móvil que tenga habilitado el servicio con cualquiera de los operadores de telefonía celular.

La conexión al dispositivo móvil que servirá de pasarela se hace a través de la librería jSMS [59] que es un API de Java para el envío y recepción de mensajes cortos (SMS) y mensajes multimedia

(MMS). Esta API soporta un amplio rango de formatos y de protocolos de comunicación, que le brinda flexibilidad a la plataforma. Por otra parte, jSMS contiene una pequeña plantilla del cliente SMTP (*Simple Mail Transfer Protocol* – Protocolo Sencillo de Transferencia de Correo) que habilita a las aplicaciones para enviar correos en Internet de acuerdo al RFC822.

El Proveedor de Correo se encarga de realizar la comunicación con el servidor de correo al cual pertenece la cuenta de correo electrónica definida por el usuario para el envío de las facturas digitales.

Para la conexión con el servidor de correo su utilizó JavaMail [60], la cual es una expansión de Java que facilita el envío y recepción de correo electrónico desde programas escritos en este lenguaje. JavaMail implementa el protocolo SMTP (*Simple Mail Transfer Protocol*) así como los distintos tipos de conexiones seguras a través de protocolos como TLS, SSL, permitiendo autentificación con usuario y clave, brindando seguridad a la plataforma.

El Proveedor de Correo debe firmar digitalmente la factura que se enviará a la cuenta de correo electrónico del usuario y para ello deberá utilizar los servicios de una autoridad de certificación, estos certificados se almacenan en un *Keystore* [61], que corresponde a un almacén de certificados y el cual se manipula a través del *Keytool* [62].

Vista de Diseño

En la Figura 25 se muestra el diagrama de paquetes de diseño de este módulo.

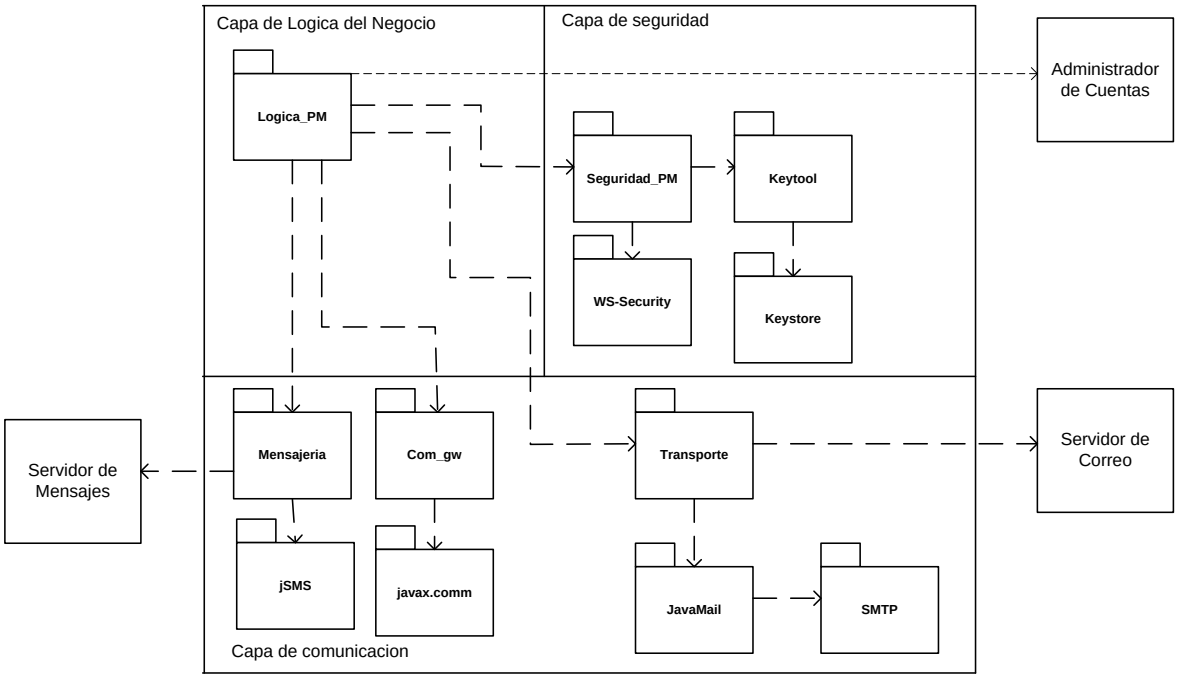


Figura 25. Paquetes de Diseño Proveedor de Mensajes

Capa de Lógica de Negocio:

- *Lógica_PM:* se refiere a la configuración necesaria para que el API de mensajería funcione, como: una licencia válida y por el puerto usb al que se conecta el móvil encargado de enviar mensajes. También contiene las clases que se encargan de fijar detalles relativos a la comunicación con el servidor de correo; como cuenta de correo del remitente y sus credenciales, dirección de correo del destino, mensaje, adjunto.

Capa de Seguridad:

- *Seguridad_PM*: tiene un manejo idéntico al acceso al Servicio Web del AC, se soporta en WS-Security para disminuir el nivel de riesgo configurando un esquema de seguridad definido en esta especificación. También asegura, a través del uso del Keystore y el Keytool, la conexión con el servidor de correo la cual se realiza mediante Java Mail.
- *WS-Security*: se refiere al esquema de seguridad empleado, que está basado en nombre de usuario, contraseña (almacenados en el servidor de aplicaciones) y clave simétrica.
- *Keytool:* hace referencia a la herramienta para manejo de certificados, que permite manipular el almacen de certificados Keystore.
- *Keystore*: se refiere al almacén de certificados que se usa para firmar la factura digital que se enviará al correo electrónico del cliente.

Capa de Comunicación:

- *jSMS:* hace referencia al API jSMS, que está escrito en Java y permite enviar diferentes tipos de mensajes sobre la red celular adaptándose perfectamente al Servicio Web que compone el Administrador de Cuentas.
- *Com_gw*: jSMS se encarga de realizar el manejo necesario del API COMM de Java, ya que se necesita de un móvil para enviar los mensajes deseados a la red celular. Al ejecutarse las clases del API acceden al móvil conectado por puerto USB.
- *Transporte:* hace referencia a todas las clases y protocolos necesarios para que un correo electrónico con la factura digital como mensaje adjunto sea enviado a la cuenta de correo del comprador. Se divide en:
  - *JavaMail:* Implementa el protocolo SMTP así como los distintos tipos de conexión con servidores de correo TLS, SSL, autentificación con usuario y contraseña.
  - *SMTP:* Se refiere al protocolo utilizado para la transferencia de correos electrónicos entre clientes y servidores.

3.3. Protocolos de comunicación

Dada la importancia de la seguridad en la comunicación entre los módulos que componen la arquitectura de facturación y pago, en la Figura 26 se han resaltado los tipos de protocolos implementados entre ellos.

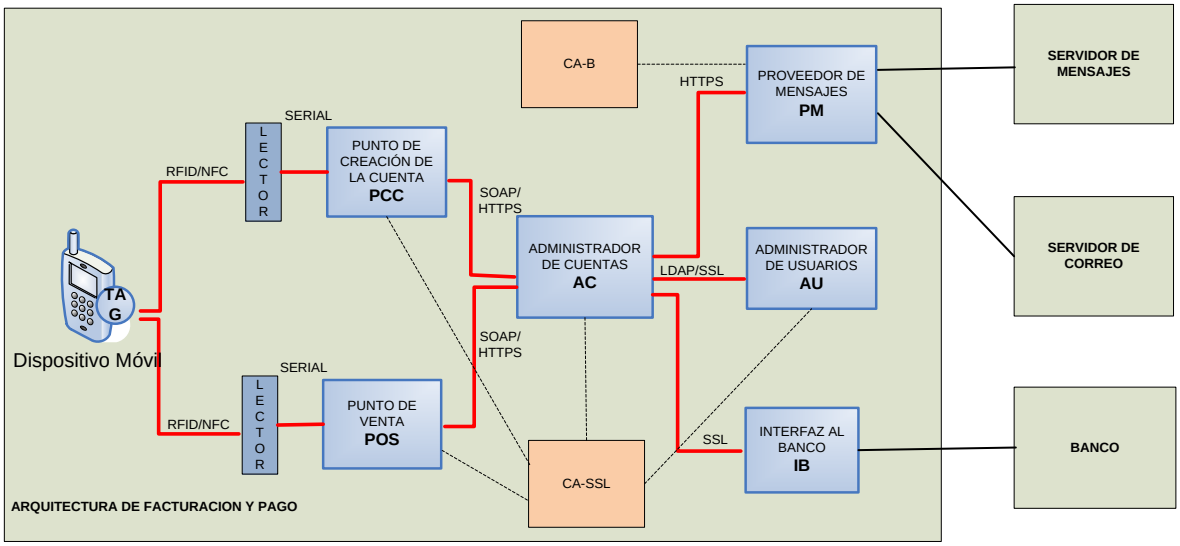


Figura 26. Protocolos de Comunicación

3.3.1. RFID/NFC

Dependiendo de la tecnología del dispositivo móvil, en este punto se puede tener ya sea el protocolo RFID o el NFC.

RFID [43]

El sistema RFID se compone de dos partes fundamentales: la etiqueta (transponder) y el lector. La etiqueta RFID está compuesta de: un micro-controlador, que a su vez consta de un procesador y una memoria; una antena (cableada o impresa con tinta de carbón conductivo) que habilita la recepción y la respuesta a solicitudes de radio-frecuencia desde un transmisor/receptor RFID, que se conoce como *transceiver*; y un material de encapsulación de polímero que envuelve la antena y el micro-controlador.

El lector inicia el proceso de identificación generando un campo RF en una frecuencia específica, definida por un sistema en particular, con lo cual causa una diferencia de voltaje por medio de un acoplamiento capacitivo o inductivo. La etiqueta detecta este cambio y después del proceso de autenticación, gracias a un mecanismo de respuesta del lector, responde transmitiendo la identificación que posee. Además del transponder y el lector, en el sistema RFID también se tiene una base de datos, donde se almacenan las características del elemento leído para realizar funciones de verificación.

La comunicación entre el lector y las etiquetas puede asegurarse por medio de algoritmos, los cuales generalmente son definidos por los fabricantes, pero se basan en estándares de cifrado como DES y 3DES.

NFC [63]

NFC es una tecnología de conectividad inalámbrica de corto rango, basada en estándares. Se basa en RFID la cual usa inducción de campo magnético para habilitar la comunicación entre

dispositivos electrónicos que se encuentren próximos. Provee un medio eficaz para la validación de los datos en protocolos de identificación.

NFC opera en la banda de frecuencia no licenciada de 13,56 MHz a distancias no mayores de 20 centímetros. Actualmente ofrece transferencia de datos de 106 kbps, 212 kbps y 424 kbps. En una comunicación NFC, un dispositivo debe tener un lector NFC y el otro debe tener una etiqueta NFC. La etiqueta es un circuito integrado que contiene datos, y que se conecta a una antena y que puede ser leído y escrito por el lector.

La comunicación NFC es *half-duplex*. Los dispositivos implementan la política "escucha antes de hablar" esto significa que todos los dispositivos deben escuchar primero la portadora y empezar a transmitir únicamente si no existe ningún otro dispositivo transmitiendo. El protocolo NFC distingue entre el iniciador y la fuente de la comunicación. Cualquier dispositivo puedes ser iniciador o fuente. El iniciador, como su nombre lo indica, es el dispositivo que inicia y controla el intercambio de datos. La fuente es el dispositivo que responde al requerimiento del iniciador.

El protocolo NFC maneja dos modos de operación: activo y pasivo. En el modo activo, ambos dispositivos generan su propio campo de radio para transmitir los datos. En el modo pasivo, únicamente uno de los dispositivos genera tal campo mientras que el otro usa modulación de carga para la transferencia. En este modo el responsable de generar el campo de radio es el iniciador. El modo pasivo de comunicación es muy importante para dispositivos que manejan baterías, como teléfonos móviles y PDAs, ya que ellos necesitan hacer un uso optimo de la energía. El protocolo NFC permite que dichos dispositivos trabajen en modo de ahorro de energía, así que la energía puede ser utilizada en otras operaciones.

La aplicación fija el valor inicial de la velocidad de la comunicación, subsecuentemente, la aplicación o el ambiente de comunicación pueden requerir adaptación de la velocidad, la cual puede ser hecha durante la comunicación. Se pueden emplear diferentes métodos de modulación y diferentes esquemas de codificación, dependiendo de la velocidad. Mientras se establece la comunicación, el iniciador inicia la comunicación en un modo particular y a una velocidad particular. La fuente entonces automáticamente determina la velocidad actual y el protocolo de bajo nivel asociado y responde de acuerdo a esto. La comunicación se termina a través de un comando de la aplicación o cuando uno de los dispositivos sale del rango.

3.3.2. Serial

El protocolo serial [47] permite la comunicación entre un PC y un lector RFID y puede ser de dos tipos, estándar y ampliado.

El protocolo serial estándar proporciona una interfaz para todos las etiquetas y los lectores iCLASS, además permite el paso de comandos para todas aquellas etiquetas que cumplan con los estándares de la ISO. El protocolo extendido permite la ejecución de comandos que habilitan que un computador se comunique con un lector que posee una interfaz de hardware USB permitiendo el control sobre el despliegue de dicho lector.

La interfaz del protocolo serial le da al computador las siguientes capacidades:

- Evitar las colisiones entre las etiquetas soportadas

- Ejecutar operaciones de lectura y escritura en las etiquetas iCLASS
- Cargar claves en el lector
- Diversificar clases para las etiquetas
- Leer y escribir la configuración del lector
- Reiniciar el campo RF del lector
- Cifrar datos con DES/3DES
- Pasar comandos a las etiquetas que estén funcionando dentro del campo RF del lector

3.3.3. SOAP

SOAP [49] es un protocolo ligero desarrollado para el intercambio de información estructurada en ambientes distribuidos descentralizados. Usa la tecnología XML para definir la infraestructura de mensajería brindando una construcción de mensajes que puede ser intercambiada sobre una gran variedad de protocolos de nivel más bajo. Para el caso de la Arquitectura de Facturación y Pago el protocolo de bajo nivel que se usara para el intercambio de los mensajes SOAP es HTTPS para garantizar la seguridad en la comunicación.

3.3.4. HTTPS

El protocolo HTTPS [64] es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las *SSL* para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. El uso del protocolo HTTPS no impide que se pueda utilizar HTTP.

Desarrollado por Netscape, SSL [65] versión 3.0 se publicó en 1996, que más tarde sirvió como base para desarrollar TLS versión 1.0, un estándar protocolo IETF definido por primera vez en el RFC 2246. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

SSL/TLS proporciona servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico y cifrando la clave de sesión mediante un algoritmo de cifrado de clave pública. La clave de sesión es la que se utiliza para cifrar los datos que vienen y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea descubierta por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. Proporciona además, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente, esta autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes.

SSL/TLS se compone de dos capas: el protocolo de registro (*Record Protocol*) y el protocolo de inicialización (*Handshake Protocol*).

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autentificación del mensaje (MAC). Cada registro tiene un campo de content_type que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo *handshake*, que tiene el content_type 22.

El cliente envía y recibe varias estructuras *handshake*:

- Envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados Challenge de Cliente o Reto). Además puede incluir el identificador de la sesión.
- Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.
- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son X.509. El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.
- Cliente y servidor negocian una clave secreta (simétrica) común llamada master secret, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función pseudoaleatoria cuidadosamente elegida.
- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes. La función pseudoaleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se vuelva vulnerables en el futuro.

3.3.5. LDAPS

LDAP [57] es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red sobre el protocolo TCP/IP. Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse, aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). LDAP esta diseñado y optimizado para ofrecer lectura y búsqueda de información a una gran cantidad de requisiciones simultáneas, sin embargo, se encuentra severamente limitado en cuanto a actualizaciones y control de transacciones en información. La actual versión de LDAP es la versión 3, la cual esta especificada en el RFC 4510.

Un cliente inicia una sesión LDAP conectándose a un servidor LDAP, por defecto a través del puerto TCP 389. El cliente envía un requerimientos al servidor y este le responde en turnos. Con algunas excepciones, el cliente podrá enviar otro requerimiento al servidor sin haber recibido la respuesta al anterior.

El cliente puede hacer los siguientes requerimientos de operaciones:

- StartTLS – Protege la conexión con el protocolo TLS para tener una conexión segura.
- Bind – Autentica y especifica la versión del protocolo LDAP
- Search – Busca y/o devuelve entradas al directorio

- Compare – Prueba si una entrada contiene un valor de atributo dado
- Add a new entry - Adicionar entradas
- Delete an entry - Borrar entradas
- Modify an entry - Modificar entradas
- Modify Distinguished Name – Mueve o renombra una entrada
- Abandon – Aborta un requerimiento previo
- Extended Operation – Operación genérica usada para definir otras operaciones
- Unbind – Cierra la conexión

Adicionalmente el servidor puede enviar "Unsolicited Notifications" que no mensajes no solicitados por el cliente ni respuestas a solicitudes.

Un método alternativo para asegurar una comunicación LDAP es usando un túnel SSL. Esto se denota en la URL utilizando el esquema ldaps. El uso de LDAPS fue común en la versión 2 de LDAP. El puerto por defecto para el uso de LDAP sobre SSL es el 636.

3.3.6.Aportes de los protocolos

A continuación se muestra una tabla resumen con los aportes y las características que los hacen posibles, de cada protocolo dentro de la arquitectura de facturación y pago.

Tabla 4. Aportes a la Arquitectura de Facturación y Pago de los Protocolos de Comunicación

PROTOCOLO	APORTES	CARACTERISTICAS
RFID/NFC	- Proximidad - Interoperabilidad - Seguridad	- Permite tener una comunicación de corto alcance, lo cual le da la característica de proximidad al sistema de pago. - Basado en estándares, permitiendo la interoperabilidad. - Implementa algoritmos para asegurar la comunicación.
SERIAL	- Acceso a datos en la etiqueta - Configuración de la comunicación - Seguridad	- Permite el acceso desde la aplicación a los datos de la etiqueta RFID, a través del lector. - Permite la configuración de la comunicación entre la etiqueta y el lector, para hacerla segura. - Permite el cifrado de la información, brindando unos niveles de seguridad adecuados.
SOAP	- Interoperabilidad	- Permite la comunicación sobre protocolos estándares, como HTTP, brindando interoperabilidad.
HTTPS	- Seguridad - Autenticación - Integridad	- Brinda seguridad en la comunicación a través del cifrado de datos basado en SSL. - Permite la autenticación, tanto de clientes como de servidores y garantiza la integridad de la información a través de una infraestructura de claves públicas.

LDAPS	- Acceso a datos almacenados - Optimización - Seguridad	- Permite el acceso a los datos almacenados en el sistema de directorio. - Optimiza el proceso de búsqueda de información, lo que permite que las operaciones de lectura de datos para la validación sean rápidas. - Ya que corre sobre HTTPS hace que el acceso a la información sea seguro.

Capítulo 4

VALIDACION DE LA ARQUITECTURA DE FACTURACION Y PAGO

La validación de la arquitectura se realizó con el fin de medir la concordancia de la misma con la definición propuesta para la plataforma de facturación y pago. Esta correspondencia y la medida de factores críticos permitieron comprobar la viabilidad de la arquitectura propuesta.

Existen diversas técnicas para la validación de las arquitecturas, en [66] se describen varias de ellas. Una de las más utilizadas es la basada en la simulación la cual utiliza una implementación de alto nivel de la arquitectura. El enfoque básico consiste en implementar los componentes de la arquitectura y, bajo un adecuado nivel de abstracción, el contexto del sistema donde va a ejecutarse. La finalidad es evaluar el comportamiento de la arquitectura bajo diversas circunstancias.

Asociada a las simulaciones se encuentra la técnica de prototipos, la cual consiste en la implementación de una parte de la arquitectura y su ejecución en el contexto del sistema. Su finalidad es evaluar los requerimientos de calidad operacional, como desempeño y confiabilidad. Para su uso se necesita una amplia información sobre el desarrollo y disponibilidad del hardware y otras partes que constituyen el contexto del sistema de software. Con esta técnica se obtiene un resultado de evaluación de mayor exactitud [67]. Dadas las características y los resultados que entrega esta técnica, fue la seleccionada para la validación de la plataforma de facturación y pago, para lo cual se desarrolló un prototipo o piloto de prueba denominado servicio SeUS.

4.1. Piloto de Prueba – Servicio SeUS

4.1.1. Caracterización de SeUS

A continuación se presentan las características más relevantes que se tuvieron en cuenta para el diseño del piloto de prueba de la plataforma propuesta.

- Por la naturaleza ubicua de SeUS el sistema de pago se realiza por proximidad y en tiempo real, lo cual es posible con el lector RFID disponible en el laboratorio de computación móvil del semillero de investigación en aplicaciones móviles e inalámbricas W@PColombia de la Universidad del Cauca.
- Con el propósito de brindar mayor flexibilidad se diseñó para que soporte tanto micro como macro pagos, sin aumentar la complejidad del sistema.
- Pensando en una implementación real del piloto, para evitar dependencia de operadores celulares y así permitir que personas y empresas ajenas a estas entidades presten el servicio

de pago móvil, SeUS se definió como un proveedor independiente de las entidades bancarias y operadores de red, ya que se establecen conexiones con estas compañías pero no se está obligado a comunicarse con una en particular. Por lo tanto, una implementación real requiere un proceso de adaptación a las particularidades del banco y realizar opcionalmente acuerdos de servicios con los operadores de telecomunicaciones.

- Con respecto al medio de pago se optó por utilizar cuentas bancarias, pero por razones técnicas y económicas, además de la dificultad en conseguir un acuerdo comercial con un banco la entidad financiera debió ser simulada en el piloto.
- SeUS utiliza tecnología RFID para transmitir los datos y credenciales de usuario, para habilitar la transacción, y mediante SMS confirma el éxito del proceso al cliente, además de enviarle la factura en formato digital al correo electrónico.

La Tabla 5 sintetiza la caracterización de SeUS.

Tabla 5. Caracterización de SeUS

Característica		**Descripción**
Ubicación del Usuario	POS	Los consumidores apuntan o pasan su móvil por un lector específico, para enviar los datos al sistema de pago, para lo cual emplean tecnología RFID o NFC.
Instante del pago	Tiempo real	Se realiza un intercambio financiero en tiempo real entre el cliente y el vendedor
Monto del pago	Micro pagos y macro pagos	Se manejan pequeñas cantidades de dinero, con ventajas como su agilidad (se procesa rápidamente) y su costo (excluye casi todos los costos adicionales que acarrean las transacciones financieras). Con alguna condición adicional (presentación del documento de identidad), también se permiten pagos de mayor cuantía.
Proveedor del Servicio	Independiente	Los usuarios de teléfonos móviles se inscriben al sistema de pago, independientemente del proveedor de telecomunicaciones, al que pertenezcan. El sistema se apoya en una entidad financiera para ofrecer un mayor respaldo en cuestiones de seguridad al usuario
Forma de pago	Basado en cuenta bancaria	El usuario autoriza que se descuente el valor de la compra de su cuenta bancaria con la gran ventaja del respaldo que ofrece una entidad financiera tanto para el vendedor como para el cliente.
Tecnologías empleadas	RFID y SMS.	Se utiliza RFID como tecnología de contacto y SMS para el envío de notificaciones

4.1.2. Requisitos funcionales y no funcionales

Los requisitos funcionales y no funcionales de SeUS se definieron con base en los definidos para la plataforma, y se describen en las siguientes tablas.

Tabla 6. Requisitos Funcionales de SeUS

REQUISITO EN LA PLATAFORMA DE FACTURACION Y PAGO	REQUISITO EN SeUS
• Crear una cuenta de servicio.	• Solicitar Creación de Cuenta. Permite al usuario crear una cuenta que lo habilite para usar el servicio de facturación y pago.
• Asociar una cuenta bancaria a la cuenta del servicio.	
• Almacenar las credenciales del usuario en el elemento seguro del dispositivo móvil.	• Grabar Etiqueta. Permitir escribir en la etiqueta toda la información referente a las credenciales del usuario.
• Almacenar la información del usuario y las credenciales en el sistema.	• Solicitar Creación de Cuenta. Permite al usuario crear una cuenta que lo habilite para usar el servicio de facturación y pago.
• Modificar la cuenta de servicio del usuario	• No se implementaron, ya que no eran relevantes para la evaluación del sistema
• Borrar la cuenta de servicio de usuario (y las credenciales del elemento seguro).	
• Informar al usuario el resultado de las acciones solicitadas.	• Notificar Resultado. Su finalidad es enviar notificaciones al usuario acerca de las acciones ejecutadas, ya sea a través de SMS o mensajes de correo electrónico, como en el caso de la factura digital.
• Activar el pago, a través de una interfaz en el dispositivo móvil.	• Realizar Pago. Permitir al usuario realizar el pago cuando se encuentra en el punto de venta.
• Hacer efectivo el pago al acercar el dispositivo móvil al lector del POS.	• Leer Etiqueta. Permitir leer en el momento del pago, la información almacenada en la etiqueta para poder hacer efectivo el pago.
• Enviar la información del pago al banco para su autorización	• Realizar Pago. Permitir al usuario realizar el pago cuando se encuentra en el punto de venta.
• Informar al usuario a través de un mensaje el resultado del proceso.	• Notificar Resultado. Su finalidad es enviar notificaciones al usuario acerca de las acciones ejecutadas, ya sea a través de SMS o mensajes de correo electrónico, como en el caso de la factura digital.
• Enviar la factura digital al correo electrónico indicado por el usuario en el momento de crear la cuenta.	

Tabla 7. Requisitos No Funcionales de SeUS

REQUISITO EN LA PLATAFORMA DE FACTURACION Y PAGO	REQUISITO EN SeUS
Seguridad	• Garantizar el monto de la transacción, que el pago se realiza únicamente una vez y el traspaso de capital se hace entre las cuentas correctas. • Seguridad en la transmisión de la información en todo el proceso de pago.
Privacidad	• Los datos sensibles del usuario no serán visibles en ningún momento durante todo el proceso
Facilidad de uso y mínima intervención del usuario	• El usuario no debe digitar claves ni realizar confirmaciones.
Espontaneidad	• El servicio se activa de manera automática.
Eficiencia	• El Vendedor debe contar con un computador que tenga conexión a Internet con disponibilidad garantizada por su proveedor de servicio, el ancho de banda y el reuso de la conexión serán los que determinen en parte el tiempo de respuesta del servicio. • El sistema garantizará rapidez en la transacción.
Flexibilidad	• El sistema permitirá trabajar en casos de desconexión de la red celular • El sistema permitirá pagos de cualquier monto, condicionando los macro pagos a la presentación por parte del usuario de alguna identificación.
Despliegue	• El sistema debe tener la capacidad de atender una cantidad considerable de usuarios.

4.1.3. Casos De Uso

En la Figura 27 se muestra el diagrama de Casos de Uso de SeUS.

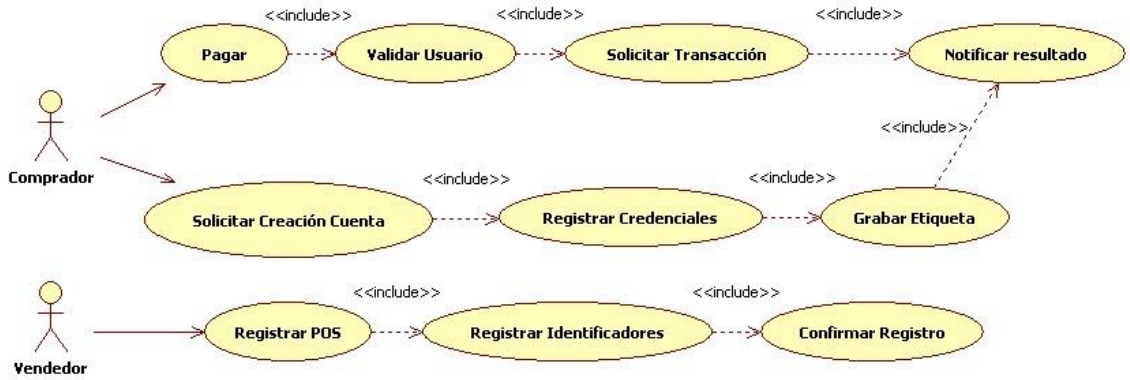


Figura 27. Diagrama de Casos de Uso

Actores

A continuación se describe el rol desempeñado los actores que aparecen en el diagrama de casos de uso de la Figura 27.

- Comprador: es el actor principal del servicio, que para usarlo debe abrir una cuenta con su información personal y necesita tener un teléfono móvil al cual asociar el servicio. Una vez se ha creado satisfactoriamente su cuenta puede pagar en el momento que desee en un POS con la infraestructura necesaria. Es el poseedor del Dispositivo Móvil de la Arquitectura de Facturación y Pago.
- Vendedor: se encarga de registrar el punto de pago para que este pueda hacer parte del servicio. Es la persona que administra el Punto de Venta de la Arquitectura.
- Administrador del Servicio: Puede llevar a cabo configuraciones importantes del servicio a través de la consola de administración del servidor de aplicaciones, corresponde al administrador de la Arquitectura.

Descripción de alto nivel

A continuación se realiza la descripción inicial de los casos de uso implementados en el piloto de SeUS.

Caso de uso	Pagar
Actores	Comprador
Impacto	Primario
Descripción	Se inicia cuando el usuario pasa su móvil con interfaz RFID en el lector del POS, con lo que se produce una solicitud de autenticación en el sistema, enviando sus credenciales desde el POS (Punto de Venta) al Administrador de Cuentas (AC) de forma segura.

Caso de uso	Validar Usuario
Actores	Comprador

Impacto	Primario
Descripción	Se inicia cuando el AC (Administrador de Cuentas) se encarga de realizar la autenticación del usuario en conjunto con el AU (Administrador de Usuarios) y permite almacenar la información de las cuentas de servicio, mediante una comunicación segura entre AC y AU.

Caso de uso	Solicitar Transacción
Actores	Comprador
Impacto	Primario
Descripción	Se inicia cuando el AC le envía al Banco, mediante una capa de adaptación, la información del comprador y vendedor para que autorice el pago a través de la cuenta bancaria registrada por el usuario.

Caso de uso	Notificar Resultado
Actores	Comprador
Impacto	Primario
Descripción	Se inicia cuando el AC solicita al Proveedor de Mensajes (PM) la notificación del resultado de una transacción y permite que el PM envié un mensaje SMS al móvil asociado por el usuario al servicio de pago, y en caso de ser necesario que envíe un correo adjuntando la factura digital, o se envié un mensaje de notificación a la aplicación que se encuentra en el POS.

Caso de uso	Solicitar Creación de Cuenta
Actores	Comprador
Impacto	Primario
Descripción	Se inicia cuando el nuevo usuario proporciona su información personal en un Punto de Creación de la Cuenta (PCC), la cual se envía al AC y permite que éste último genere las credenciales necesarias para el nuevo usuario. La comunicación entre PCC y AC se realiza de forma segura.

Caso de uso	Registrar Credenciales
Actores	Comprador
Impacto	Primario
Descripción	Se inicia cuando el AC genera la contraseña del usuario y permite su registro adicional a la información que la persona introdujo, en una nueva cuenta de servicio en el AU, mediante una comunicación segura entre AC y AU.

Caso de uso	Grabar Etiqueta

Actores	Comprador
Impacto	Primario
Descripción	Se inicia cuando el AC envía al PCC las credenciales y estas se graban en la etiqueta RFID y permite que el usuario pueda acceder al servicio mediante el lector del POS.

Caso de uso	Registrar POS
Actores	Vendedor
Impacto	Primario
Descripción	Se inicia cuando el vendedor envía al AC la información necesaria para crear una cuenta mediante la aplicación del POS, mediante una comunicación segura entre POS y AC.

Caso de uso	Registrar Identificadores
Actores	Vendedor
Impacto	Primario
Descripción	Se inicia cuando el AC envía la información del punto de venta para que se registre en el AU. y se le envía al vendedor una confirmación de la operación realizada.

Caso de uso	Confirmar Registro
Actores	Vendedor
Impacto	Primario
Descripción	Se inicia cuando el AC solicita al PM la notificación al vendedor del resultado del proceso de creación de la cuenta de servicio con un mensaje en la aplicación del POS, y permite que pueda recibir pagos en su establecimiento.

Descripción Detallada del Caso de Uso Pagar

Pagar	
ACTOR:	Comprador
PROPOSITO:	Efectuar el pago de artículos mediante una interfaz de proximidad.
RESUMEN:	Inicia cuando el comprador pasa el móvil por el lector del POS, en ese momento se transmiten las credenciales de seguridad, almacenadas en la etiqueta al lector y luego del POS al AC, que obtiene la información de cuenta bancaria del usuario comunicándose con el AU, para conectarse con el Banco y enviarle la información necesaria para realizar la transacción. Finalmente se notifica al usuario y al POS si la transacción fue exitosa o únicamente a éste último si ocurrió algún error.
PRECONDICIONES:	• El móvil debe contar con interfaz RFID, el POS debe contar con conectividad a red. • Se deben generar o comprar los certificados necesarios en el AC y

	AU. • Se debe fijar las rutas de acceso a los certificados en los dos módulos mencionados. • Se debe fijar la información de acceso al Servidor de Directorio del AU, como dirección ip y puerto. • El usuario ha realizado un proceso previo de los artículos que va a adquirir.
ESCENARIO	Comprador 1. La etiqueta asociada al móvil se pasa por el lector y se realiza autenticación mutua entre ambos E1. 2. Se transmiten las credenciales almacenadas en la etiqueta. 3. Las credenciales se transmiten desde el POS al AC, E2. 4. Se fijan las rutas de acceso los certificados necesarios E3. 5. Petición de autenticación por parte del AC al AU, para el usuario que desea pagar. E4 6. Extraer información de cuentas bancarias alojadas en la cuenta de servicio en el AU. 7. Conexión con el Banco para solicitar que se efectúe la transacción. E5 8. Notificar resultado al POS. 9. Generación y envío de SMS al móvil del comprador. 10. Generación y envío de la factura digital a la cuenta de correo del comprador.
POSCONDICIONES:	Compra realizada
FLUJOS ALTERNATIVOS:	Ninguno
NOTAS:	Ninguna
EXCEPCIONES:	E1: No se puede realizar Autenticación Mutua. - No hay transferencia de credenciales. E2: El Cliente de Servicio no puede autenticarse. - No se puede establecer comunicación con el AC. E3: No se puede realizar comunicación sobre SSL. - No hay transferencia de credenciales. E4: La cuenta fue eliminada o suspendida. - El usuario es rechazado. E5: La red del Banco no está disponible. - Es imposible realizar la transacción.

Diagrama de Clases Caso de Uso Pagar

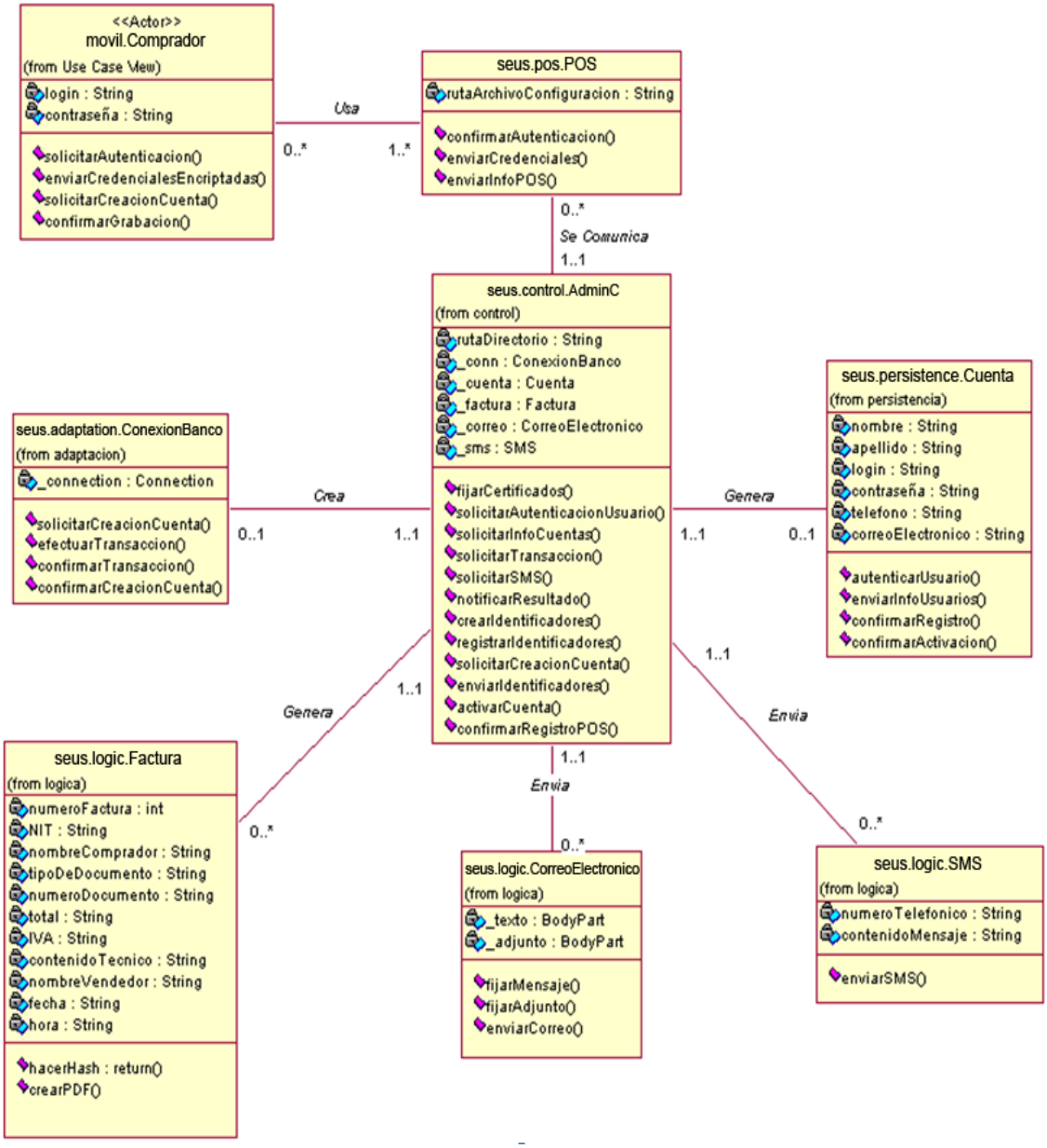


Figura 28. Diagrama de Clases del Caso de Uso Pagar

Diagrama de Secuencia caso de Uso Pagar

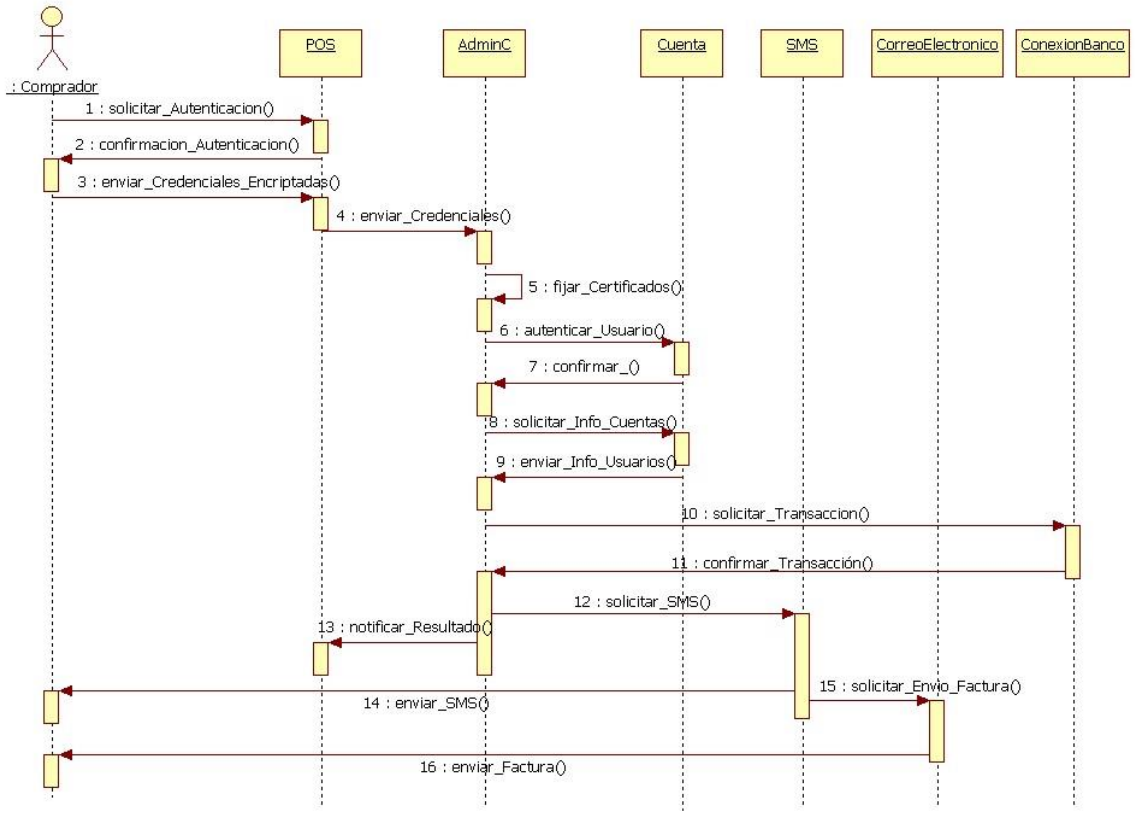


Figura 29. Diagrama de Secuencia del Caso de Uso Pagar

La descripción detallada de los demás casos de uso se encuentra en el Anexo A.

4.2. Implementación de SeUS

La Figura 30 muestra el diagrama de implantación del piloto de SEUS. Las flechas azules ilustran las comunicaciones realizadas sobre protocolos seguros y las blancas relaciones directas, donde no hay un protocolo de comunicación involucrado. A continuación, se describe cada componente.

La implementación de SeUS se constituye en la instanciación física de la plataforma de facturación y pago, por tanto los módulos que hacen parte de SeUS se basan en los definidos para la arquitectura, aunque para hacer un mejor uso de los recursos computacionales varios módulos funcionales de la aplicación se implantaron sobre el mismo servidor físico.

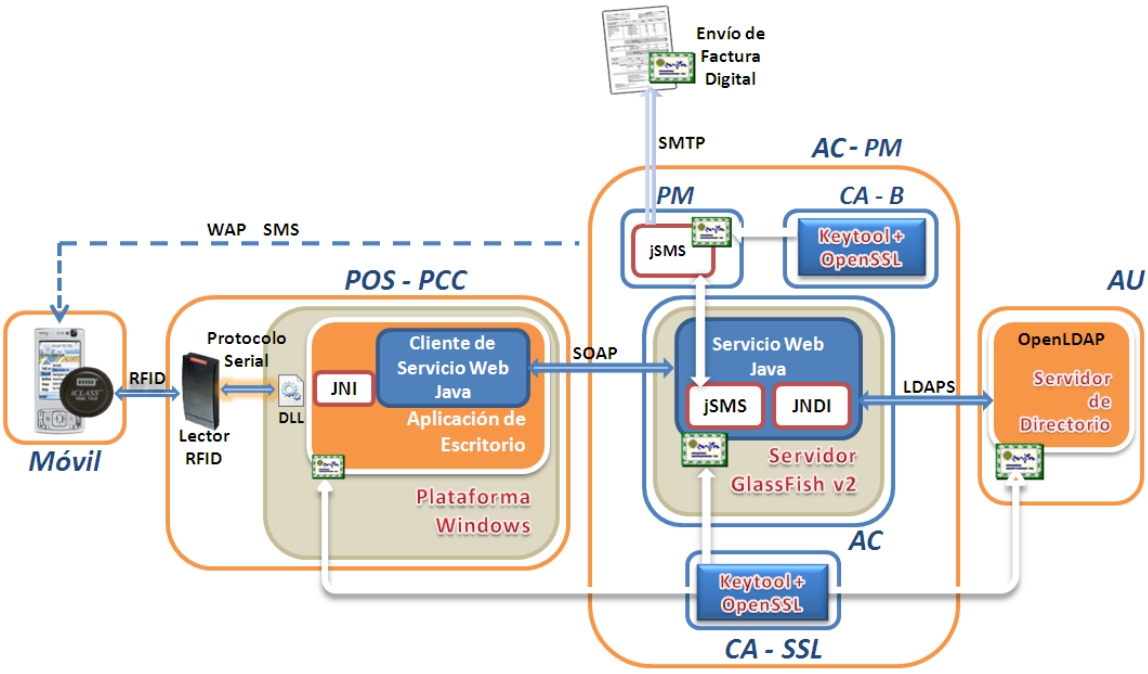


Figura 30. Diagrama de Implantación

4.2.1.AC-PM

AC

El AC se compone de un Servicio Web seguro implementado en Java, se desplegó en el Servidor de Aplicaciones GlassFish v2, el cual tiene como parte fundamental METRO [68], que es un web services stack compuesto por una implementación del api JAX-WS (XML-Based Web Services (JAX-WS) 2.0) [69].

El servidor se implantó en una estación con Sistema Operativo Debian Etch 4.0 y Java 2 SE. Estas decisiones de implementación se basaron en las siguientes consideraciones:

- Se utilizó Debian Etch 4.0 un sistema operativo muy seguro y estable [70]. Es además una de las distribuciones de Linux más populares [71] por lo cual dispone de soporte en muy poco tiempo mediante foros y listas de correo.
- Se utilizó Java(TM) 2 *Runtime Environment, Standard Edition* (build 1.5.0_14-b03), debido a que al momento de implementación era la última versión de JavaSE considerada estable en Linux Debian.
- Se empleó GlassFish v2 [72], como servidor de aplicaciones, el cual implementa características de Java EE 5 como JSP (Java Server Pages) 2.1, JSF (Java Server Faces) 1.2, Enterprise JavaBeans 3.0, entre otras tecnologías, pero en particular, lo que lo hace idóneo para ser usado en SeUS, es el soporte para esquemas de seguridad que posee, ya que Metro (parte del núcleo de Glassfish) implementa la especificación WS-Security 1.0 y 1.1, el cual se usó junto con SSL para incrementar el nivel de seguridad.
- El Servicio Web desarrollado hace uso del api JNDI, para utilizar el Protocolo LDAP sobre SSL, que se denomina LDAPS. El Servicio Web se comunica con sus clientes mediante el protocolo SOAP 1.1, definido en [73], que tiene como base XML v1.0 y viaja sobre HTTP.

- Debido a que el banco se simuló como una base de datos de MySQL 5.0, la capa de adaptación del AC con el Banco se realizó con DAO mediante FREE DaoGen generator versión 2.4.1 [74].

PM

Al usuario se le envían mensajes de notificación con los resultados de las operaciones realizadas, los cuales son de tipo SMS, para esto se utilizó ObjectXP jSMS 2.2.1. jSMS es un API escrita en Java, que luego de una sencilla configuración se puede usar como interfaz para el desarrollo de aplicaciones de mensajería, , y que se integra muy fácilmente con el Servicio Web seguro del AC.

jSMS 2.2.1 también se utilizó para el envío de la factura digital firmada a la cuenta de correo del usuario luego de realizar una compra.

CA-SSL y CA-B

Las herramientas para realizar la generación de certificados, llaves y keystores son Java Keytool y OpenSSL 0.9.8c.

4.2.2.AU

Es el servidor que almacena toda la información de cuentas de usuario del servicio. Es un servicio de directorio montado con OpenLDAP-2.3.39, corriendo sobre una estación con Debian Etch 4.0 y que se comunica con el AC a través de LDAPS, el cual consiste en la implementación del protocolo LDAP sobre SSL. OpenLDAP ofrece características muy deseables para almacenar la información de los usuarios de un servicio de pago, como robustez y velocidad en lectura de información. Implementa el protocolo LDAP v3 [75], aunque tiene compatibilidad hacia. Se define también la ruta donde OpenLDAP guarda su directorio en una base de datos de tipo Oracle Berkeley, la versión estable para realizar la compilación fue la 4.4.

4.2.3.POS – PCC

Es el último servidor empleado en el cual se montaron tanto el Punto de Creación de cuentas y el Punto de Pago, que se describen a continuación:

Punto de Venta – Punto de Creación de Cuentas

El POS y el PCC están montados bajo el mismo esquema, que se puede resumir como Debian Etch, JavaSE y una aplicación Java de escritorio, que cuenta con la característica de ser un Cliente de Servicio Web seguro y comunicarse con un lector RFID del fabricante HID cuya referencia es iCLASS RW100/6101 BKV000, como se había definido en la etapa de diseño de la arquitectura.

La aplicación Java de escritorio, que se implementa en estos módulos, se comunica con el lector RFID mediante la implementación del Protocolo Serial iCLASS v2.4 a través de un puerto USB, esta comunicación se lleva a cabo utilizando el API JNI gracias a la cual la aplicación de escritorio puede acceder a métodos nativos escritos en lenguaje C que se encuentran en una librería dinámica (DLL *Dynamically Linked Library*).

La aplicación de escritorio del POS requiere de un archivo de configuración, que almacena información de la cuenta de servicio y la cuenta bancaria asociada al establecimiento que tiene el POS.

4.2.4. Móvil

Como se explicó en el numeral 3.2.2.3.1., RFID HF es la mejor opción para un sistema de pago móvil, al manejar etiquetas con mayor capacidad de almacenamiento, más económicas, que pueden ser fácilmente embebidas en otros artículos y que permiten una alta tasa de transmisión de datos a distancias cortas; además de contar con estándares consolidados como el ISO 14443, que garantizan interoperabilidad entre dispositivos. NFC también es una opción en un sistema de pago móvil, si se tiene en cuenta que es una mejora de RFID HF en aspectos como seguridad y la tasa de transferencia, pero conservando características como la frecuencia de operación. Debido a los recursos tecnológicos con que se cuenta en la Universidad, se optó por emplear una solución con RFID HF, que garantiza las características de ubicuidad que se pretenden en la solución y permite una integración futura con dispositivos y sistemas NFC.

En el mercado existen diversas opciones de equipos RFID. Por su costo y características una opción sobresaliente es el lector RW100 de HID que puede leer y escribir información en etiquetas RFID trabajando en la frecuencia de 13.56MHz. Este equipo es capaz de cifrar los datos transmitidos con algoritmos seguros y estandarizados como son 3-DES y realizar autenticación mutua con la tarjeta o etiqueta RFID, además de ser compatible con los estándares más populares de tarjetas de contacto cercano como son ISO 15693 e ISO14443B con los cuales cumple la etiqueta iCLASS tag 206X escogida para el piloto de SeUS [76].

4.3. Validación de los Requisitos Funcionales

La validación del cumplimiento de los requisitos funcionales de la arquitectura básicamente depende de la implementación realizada en el piloto de prueba y de su funcionamiento. En la siguiente tabla se muestra el resultado de dicha evaluación.

Tabla 8. Validación de los Requisitos Funcionales

REQUISITO DE LA PLATAFORMA DE FACTURACION Y PAGO	REQUISITO DE SeUS	CUMPLIO
• Crear una cuenta de servicio. • Asociar una cuenta bancaria a la cuenta del servicio.	• Solicitar Creación de Cuenta. Permite al usuario crear una cuenta que lo habilite para usar el servicio de facturación y pago.	SI
• Almacenar las credenciales del usuario en el elemento seguro del dispositivo móvil.	• Grabar Etiqueta. Permitir escribir en la etiqueta toda la información referente a las credenciales del usuario.	SI
• Almacenar la información del usuario y las credenciales en el sistema.	• Solicitar Creación de Cuenta. Permite al usuario crear una cuenta que lo habilite para usar el servicio de facturación y pago.	SI

• Modificar la cuenta de servicio del usuario • Borrar la cuenta de servicio de usuario (y las credenciales del elemento seguro).	• No se implementaron, ya que no eran relevantes para la evaluación del sistema	SI
• Informar al usuario el resultado de las acciones solicitadas.	• Notificar Resultado. Su finalidad es enviar notificaciones al usuario acerca de las acciones ejecutadas, ya sea a través de SMS o mensajes de correo electrónico, como en el caso de la factura digital.	SI
• Activar el pago, a través de una interfaz en el dispositivo móvil.	• Realizar Pago. Permitir al usuario realizar el pago cuando se encuentra en el punto de venta.	SI
• Hacer efectivo el pago al acercar el dispositivo móvil al lector del POS.	• Leer Etiqueta. Permitir leer en el momento del pago, la información almacenada en la etiqueta para poder hacer efectivo el pago.	SI
• Enviar la información del pago al banco para su autorización	• Realizar Pago. Permitir al usuario realizar el pago cuando se encuentra en el punto de venta.	SI
• Informar al usuario a través de un mensaje el resultado del proceso. • Enviar la factura digital al correo electrónico indicado por el usuario en el momento de crear la cuenta.	• Notificar Resultado. Su finalidad es enviar notificaciones al usuario acerca de las acciones ejecutadas, ya sea a través de SMS o mensajes de correo electrónico, como en el caso de la factura digital.	SI

Como se puede observar de la Tabla 8 se concluye que todos los requisitos definidos para la plataforma de facturación y pago se pudieron implementar en el prototipo y que por tanto se puede decir que los requerimientos funcionales son todos factibles de implementación.

4.4. Validación de los Requisitos No Funcionales

La validación de los requisitos no funcionales se constituye en una tarea bastante complicada [77], puesto que se pretende medir propiedades del sistema con base en especificaciones abstractas. Por ello, la intención es más bien la evaluación del potencial de la arquitectura diseñada para alcanzar los atributos de calidad requeridos.

Las mediciones que se realizan para evaluar los distintos parámetros pueden tener diferentes objetivos [66] dependiendo del contexto de la implementación y de las técnicas empleadas para hacer la medición. Estos objetivos son tres: cualitativos, cuantitativos y máximos y mínimos teóricos.

La medición cualitativa brinda respuestas afirmativas o negativas, sin mayor nivel de detalle. Puede resultar de la comparación entre tecnologías existentes con el fin de determinar las mejores opciones relacionadas con ciertos atributos. La medición cuantitativa busca la obtención de valores que permitan tomar decisiones en cuanto a los atributos de calidad de una arquitectura de software. El esquema general es la comparación con márgenes establecidos, como lo es el caso de los requerimientos de desempeño, para establecer el grado de cumplimiento de una arquitectura candidata, o tomar decisiones sobre ella. Este enfoque permite establecer comparaciones, pero se ve limitado en tanto no se conozcan los valores teóricos máximos y mínimos de las mediciones con las que se realiza la comparación. Por último, la medición de máximo y mínimo teórico contempla los valores teóricos para efectos de la comparación de la medición con los atributos de calidad especificados. El conocimiento de los valores máximos o mínimos permite el establecimiento claro del grado de cumplimiento de los atributos de calidad [66].

A continuación se relacionan cada una de las técnicas empleadas y los resultados obtenidos para evaluar cada uno de los requisitos no funcionales de la arquitectura, basados en el comportamiento del prototipo implementado.

4.4.1. Seguridad y Privacidad

Dada la importancia de estas características dentro de la arquitectura de facturación y pago el proceso de evaluación de las mismas se hizo de una manera más rigurosa siguiendo una metodología estándar como se describe en [11]. En la Tabla 9 se presentan las etapas de la metodología seguida.

Tabla 9. Metodología para las pruebas de seguridad

METODOLOGÍA DE GESTIÓN DE SEGURIDAD EN SeUS	
PLAN – Establecer ISMS (*Information Security Management System* - Sistema de Gestión de seguridad de Información)	• Definir alcance y límites de ISMS. • Identificar activos del servicio. • Identificar personal vinculado al servicio.
	Modelado de Amenazas OWASP (Open Web Application Security Project)
	• Identificar amenazas. • Valorar amenazas.
	• Plantear Políticas de Seguridad.
DO – Implementar y Operar	• Generar un ambiente que permita la simulación de la amenaza y emplear la contramedida propuesta para la

ISMS	misma.
CHECK – Monitorear y Revisar ISMS	• Evaluar los resultados obtenidos con los esperados, y determinar la eficacia de las medidas adoptadas para cada una de las amenazas.
ACT – Mantener y Mejorar ISMS	• Corregir los errores detectados en el paso anterior y llevar a cabo las mejoras necesarias.

Un aspecto importante dentro del proceso escogido consistió en la selección de las amenazas y su valoración con base en criterios como el impacto de la amenaza en el servicio y la facilidad de ejecución de la misma. En la Tabla 10 y Tabla 11 se describen las escalas utilizadas.

Tabla 10. Valoración del Impacto

Valoración	Descripción del grado de impacto
5	Alto
4	Moderado
3	Medio
2	Bajo
1	Insignificante

Tabla 11. Facilidad de ejecución de la amenaza

Valoración	Grado de Facilidad
5	Bajo: No se requiere ningún conocimiento, el ataque o daño se lleva a cabo de forma intuitiva y espontánea.
3	Medio: Para que ocurra el daño se requiere algún conocimiento y de herramientas asequibles.
1	Muy difícil, casi imposible: Para llevar a cabo la amenaza se requiere un conocimiento alto y varias herramientas

Las amenazas identificadas en el piloto SeUS se describen a continuación:

- Suplantación de usuarios, donde intrusos realicen transacciones en nombre de clientes registrados en el sistema (clonar etiquetas, acceder al servidor del AC, y pérdida, robo o uso sin autorización del móvil).
- Acceso por parte de extraños a la información de usuario almacenada en el directorio del AU.
- Inserción de datos al directorio del AU por parte de intrusos.
- Interceptación de información.
- Suplantación de equipos de SeUS, en especial los servidores.
- Ataques que desactiven servidores y desencadenen fallas en la prestación del servicio (Ataques al AC y al AU).
- Negación de la transacción por parte del usuario o por parte del vendedor.
- El correo electrónico con la factura digital no llega al correo del usuario.
- El SMS de confirmación no llega al usuario.

- No llega el mensaje de confirmación al vendedor o toma mucho tiempo.

Teniendo en cuenta los criterios de valoración definidos, las amenazas detectadas se clasificaron como se muestra en la Tabla 12.

Tabla 12. Clasificación de las amenazas

Descripción de la Amenaza	Impacto	Facilidad	Servicio de seguridad que afecta la amenaza	Contramedida
Suplantación por clonación de etiquetas.	5	1	Autenticación	- Usar tecnología RFID que imposibilite la clonación. - Hacer de la grabación de claves, en la etiqueta RFID, un proceso totalmente seguro y privado.
Suplantación por robo, pérdida o uso no autorizado	4	5	Autenticación	- Educar al usuario en el cuidado de su móvil. - Habilitar una línea telefónica que permita la desactivación inmediata de la cuenta de usuario. -Solicitar un documento en el momento del pago. - Implementar lectores RFID con reconocimiento de huella dactilar. (En SeUS se implementó sin huella dactilar porque el lector disponible en la Universidad carece de esta tecnología)
Suplantación de un punto de pago o de un punto de creación de cuentas.	4	1	Autenticación	- Utilizar mecanismos de seguridad entre el Servidor Web del AC y el cliente del Servicio Web del POS y PCC.
Acceso de intrusos a la información del directorio de usuarios / Inserción de datos al directorio de usuarios	5	1	Confidencialidad, Autenticación, Integridad.	- Herramientas de protección para el Administrador de Usuarios como un firewall. - Educar al Administrador de Usuarios para que maneje de forma eficiente y confidencial la información. - Utilizar contraseñas que dificulten el éxito de un ataque de fuerza bruta. - Establecer listas de Control de acceso para los usuarios. - Restringir el acceso físico a los servidores.
Interceptación de información	4	1	Confidencialidad, Autenticación, Integridad.	- Cifrar la información transmitida. - Utilizar mecanismos que permitan la autenticación entre entidades de SeUS, como VPN.

Suplantación de equipos de SeUS, en especial los servidores.	5	1	Confidencialidad, Autenticación, Integridad.	- Utilizar mecanismos que permitan la autenticación entre entidades de SeUS, como VPN.
Ataques que desactiven servidores y desencadenen fallas en la prestación del servicio.	5	1	Integridad, Autenticación	- Utilizar herramientas de protección para el Servidor de cuentas y el de Usuarios, como firewalls. - Usar redundancia en los servidores.
Negación de la transacción por parte del usuario o por parte del vendedor.	2	5	No repudio	- Entregar una factura digital firmada al usuario. • Llevar un registro de las transacciones en el sistema. - Ubicar cámaras Web en el POS, y llevar un registro con fotografías de los compradores.
El correo electrónico con la factura digital no llega al correo del usuario	2	3	Integridad, No repudio	- Acuerdos de calidad de servicio entre SeUS y el Servidor de Correo.
El SMS de confirmación no llega al usuario.	2	3	Integridad, No repudio	- Acuerdos de calidad de servicio entre SeUS y el operador celular.
No llega el mensaje de confirmación al vendedor o toma mucho tiempo.	3	3	Integridad, No repudio	- Hacer un estudio de recursos adecuado en la conexión y ancho de banda en el momento de desplegar al servicio.

Como puede verse de la tabla anterior, las amenazas pueden clasificarse en dos tipos, amenazas que dependen de las características técnicas de la arquitectura y las amenazas que dependen de las políticas de seguridad definidas en todas las entidades que intervienen en el sistema para el manejo de todo el proceso de facturación y pago.

A continuación se describen las pruebas de seguridad relacionadas con los aspectos técnicos que se realizaron a la arquitectura a través de SeUS.

Para llevar a cabo las pruebas de seguridad en primer lugar se deben conocer los tipos de ataques que puede sufrir una red, donde sobresalen: Búsqueda (scanning), escucha (sniffing), suplantación (spoofing), denegación del servicio (denial of service) y códigos maliciosos (exploits) [78]:

- Búsqueda: Los ataques de scanning consisten en identificar los puertos que están escuchando en la red, y que pueden representar un punto vulnerable de un equipo. Generalmente constituyen el primer paso de un ataque.
- Escucha: Consiste en recopilar información de la red, por lo cual se considera un ataque pasivo, donde se intenta violar la privacidad y confidencialidad de las comunicaciones.
- Suplantación: Conocido como ataque de autenticación, donde se intenta engañar al sistema al tomar la identidad de un usuario con privilegios.

- Denegación del servicio: Consiste en impedir el acceso de los usuarios a un servicio, mediante saturación de solicitudes al servidor, pérdida de la conectividad o sobrecarga de datos en el enlace.
- Códigos maliciosos: Consisten de programas denominados exploits, que se ejecutan local o remotamente y que explotan las vulnerabilidades de un equipo.

La Topología de la red utilizada para las pruebas es la mostrada en la Figura 31, en donde se emplearon 3 equipos para la simulación del servicio y otro más para realizar los ataques.

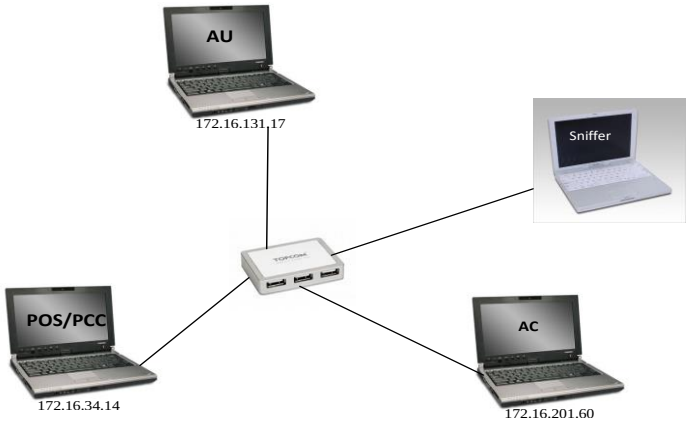


Figura 31. Topología de la red de pruebas

Basado en los posibles ataques se desarrollaron pruebas en los siguientes aspectos:

- Pruebas de scanning. Estas pruebas permiten detectar los puertos abiertos en un equipo. Este análisis se realizo a los servidores AC y AU y aunque es un procedimiento pasivo e inofensivo, permitió detectar la facilidad con la cual se accede a ese tipo de información y que después puede convertirse en el primer paso de un ataque que concluya con la deshabilitación de cualquiera de los dos servidores. Por lo anterior es importante y fundamental instalar un firewall que impida este tipo de ataques y así bloquear cualquier tipo de amenaza desde el principio. Después de hacer la instalación del firewall y realizar el scanning se ve que ya no es posible visualizar los puertos abiertos.
- Pruebas de sniffing. Estas pruebas permiten el monitoreo y análisis del trafico que se cursa en el sistema. Al capturar la información que se transmite entre el AC y el AU se pudo observar que esta información estaba cifrada, haciendo imposible visualizar los datos transferidos y las operaciones que se llevan a cabo, debido al manejo de certificados y del protocolo TLS en el Servidor. El mismo tipo de pruebas se realizaron entre el AC y el POS/PCC. La prueba realizada consistió en crear una nueva cuenta de vendedor, y monitorear el proceso con el sniffer obteniéndose que los datos pasan cifrados y son imposibles de entender.
- Pruebas de spoofing. El spoofing es una técnica de ataque consistente en suplantar a una entidad de una red con el fin de recibir información confidencial. Las dos entidades escogidas para esta prueba fueron el AC y el AU, y se utilizo una herramienta que permitió la suplantación del AU. Al hacer la prueba se detectó que a pesar de que la información se transmite de manera cifrada, el suplantador además de interceptar los datos, los recibe incluyendo llaves de seguridad, por lo cual con las herramientas y algoritmos suficientes se podría descifrar la información. Este no es un proceso sencillo y por el contrario requiere la

intervención de un experto, sin embargo representa un riesgo para el sistema, por lo que se debe implementar una solución que permita una comunicación segura basada en una autenticación previa de las entidades involucradas en ella. En SeUS se implementó una VPN que impide la conexión de intrusos a equipos del servicio al solicitar una autenticación inicial.

- Pruebas de denegación de servicio. En muchas ocasiones el atacante no tiene el conocimiento y las herramientas para descifrar la información, entonces opta simplemente por interrumpir la comunicación y así alterar la prestación del servicio, esta prueba que fue llevada a cabo en SeUS para ello se intentó acceder al directorio LDAP del AU desde el AC y el resultado fue el no acceso al servidor. También se realizo la inserción de datos en la comunicación, facilitando la generación de una sobrecarga en el enlace, que es otra forma de ataque de Denegación del servicio. Aunque el desenlace es diferente al del ataque spoofing, el origen es el mismo, la ausencia de un mecanismo robusto de autenticación que impida la suplantación de una entidad, por lo cual la solución también es una VPN.
- Pruebas de exploits. Un exploit es un programa que aprovecha una vulnerabilidad de un equipo para alterar el funcionamiento de un servicio o aplicación. Al realizar el ataque a los servidores AC y AU de SeUS se obtuvieron buenos resultados de seguridad, es decir ninguno de los exploits tuvo éxito. Pero, así actualmente no se encuentren exploits que afecten a SeUS, en cualquier momento puede aparecer una amenaza para este sistema, por lo cual es importante evitar este tipo de ataques, la solución la provee el firewall ya instalado en los servidores, el cual impide la detección de los servidores por parte de los programas de exploits.

La descripción detallada de todas las pruebas se encuentra en el Anexo B.

4.4.2. Mínima intervención del usuario

Para determinar esta característica en la arquitectura se realizó una medida cualitativa del servicio SeUS, comparándolo con sistemas de pago existentes y de gran aceptación entre los usuarios, ya que este factor es un aspecto determinado en gran parte por la experiencia de cada individuo al momento de usar el servicio, y es algo difícil de percibir por los desarrolladores.

Si se tienen en cuenta el grado de aceptación de las tarjetas de crédito por parte de los usuarios [79] y las mejoras que un sistema de pago móvil presenta frente a estas formas de pago tradicionales, se puede garantizar en gran medida la mínima intervención del usuario en el momento de usar el servicio de SeUS. Al no ser necesario llevar consigo una tarjeta, ni digitar claves en equipos extraños se mejora la experiencia del usuario final que percibe el servicio como fácil de utilizar.

4.4.3. Espontaneidad

SEUS es espontáneo, ya que los usuarios lo pueden iniciar en cualquier momento, en alguno de los puntos de venta, una vez han creado una cuenta en el sistema. Al incurrir todo el proceso de pago en tiempos cortos de duración es poco probable que el cliente entable una relación de larga duración con el sistema en el momento del pago.

4.4.4. Eficiencia

Al hablar de eficiencia en un servicio de pago, se considera el tiempo o duración de la transacción, razón por la cual la evaluación de esta característica se realizó de manera cuantitativa. La idea de la medida es evaluar el tiempo desde que el usuario inicia el proceso pasando el dispositivo móvil por el lector en el punto de venta hasta que recibe la notificación del resultado de la transacción y la factura digital.

Para poder tener una medida acertada del tiempo que demora la arquitectura de facturación y pago en realizar todo el proceso es necesario tener en cuenta el momento en el cual ella deja de ser la responsable del proceso y empiezan su intervención otros agentes como el proveedor del servicio de telefonía celular, para el envío de los mensajes de texto, y el proveedor del servicio de Internet para el envío de la factura digital.

De acuerdo a lo anterior para el caso de SeUS se considera que el tiempo de envío termina una vez se ha enviado el correo electrónico con la factura digital, y el SMS de confirmación de la transacción al móvil del cliente, desde los módulos Proveedor de Correo y Proveedor de Mensajes. Retrasos por fallas en la red celular, por estar el dispositivo móvil apagado o por inconvenientes con la cuenta de correo del cliente no son responsabilidad de SeUS y no se contabilizan en el tiempo del servicio.

Para determinar la eficiencia de SeUS se hicieron medidas del tiempo de procesamiento de la información y la memoria consumida. Estas se tomaron a los módulos AC y POS/PCC y se detallan en el Anexo B. Los resultados obtenidos fueron los siguientes:

Módulo AC.

- Procesamiento de la información: El tiempo máximo que tarda el servicio Web para empezar a atender solicitudes, una vez compilado, es 45.2 ms.
- Consumo de memoria: Una vez lanzado el servicio, el consumo de memoria empieza a crecer alcanzado un pico de 50 Megas, pero en un tiempo aproximado de 40 segundos el consumo se estabiliza en 30 Megas, que es un valor bastante bajo respecto a la memoria disponible. Cuando el PCC o el POS requieren un servicio (creación de cuentas y realización de pagos) se presenta un leve aumento en el consumo de memoria.

Módulos POS/PCC

- Procesamiento de la información: Los tiempo de procesamiento del POS y del PCC son aproximadamente 700 ms y 3000 ms. El tiempo de inicialización del POS es significativamente mayor que el tiempo del PCC ya que al inicializarse realiza una conexión de prueba con el AC, que no se lleva a cabo al ejecutar la aplicación del PCC.
- Consumo de memoria: Tanto el PCC como el POS son clientes del servicio Web, por lo cual tienen poco procesamiento y consecuentemente bajo consumo de memoria.

Con base en las pruebas realizadas se puede concluir que el proceso de pago es corto, de aproximadamente 10 segundos, debido a las propiedades de las tecnologías y herramientas empleadas, convirtiéndolo en un sistema con tiempos de transacción comparables a los de sistemas de pago tradicionales como el de tarjetas débito o de crédito, con una ventaja en la

manera como se ejecuta el proceso en el instante de pago, ya que con SeUS este proceso es mucho más corto ya que solo requiere pasar el dispositivo móvil cerca al lector en el punto de pago.

4.4.5. Flexibilidad

La evaluación de la flexibilidad se basa en una medida cualitativa resultado de la comparación con otros sistemas de pago. Un aspecto importante relacionado con esta característica es el tipo de pagos que se permiten, con SeUs se puede ver que en la arquitectura se posibilita la realización tanto de micropagos como macropagos.

Para transacciones de bajo valor lo más importante es tener un proceso ligero y rápido, por lo cual SeUS permite pagos menores a 20000 pesos con solo pasar el teléfono celular por el lector de RFID. En transacciones de un valor más alto el aspecto más relevante es la confianza que debe existir entre el usuario y el proveedor del servicio, por lo cual SeUS solo autoriza el pago con la presentación del documento de identidad antes de realizar la transacción, una vez se ha pasado el teléfono celular por el lector de RFID.

Este es un aspecto que ya depende de las políticas del almacén, pero a nivel tecnológico puede verse que la arquitectura permite los dos tipos de pago, brindando flexibilidad en este aspecto.

La naturaleza ubicua de SeUS lo hace un sistema flexible frente a otras formas de pago tradicionales, incluso al considerar el caso de operación desconectada que es tan importante en un entorno ubicuo, ya que el pago se puede realizar en un POS independientemente de si el móvil del usuario se encuentra en una zona cubierta por la red celular, solo se afecta el tiempo de recepción de los mensajes de notificación

4.4.6. Despliegue

Debido a que los servicios ubicuos cuentan con características de los servicios distribuidos, en SeUS es sencillo atender usuarios en un lugar diferente mediante la creación de nuevos puntos de pago y/o de creación de cuentas para prestar el servicio a más personas. Además se han usado herramientas robustas como un servidor de aplicaciones de alta capacidad como Glassfish y un servicio de directorio muy estable como OpenLDAP, que además de ser libres no implican costos adicionales en software a la hora de ampliar la cobertura con más puntos de pago.

SeUS además de permitir la ampliación en la cobertura del servicio de facturación y pago con el establecimiento de nuevos puntos de venta, también facilita la incorporación e interacción del sistema con otros servicios, gracias a la flexibilidad e interoperabilidad que ofrece un servicio Web y el diseño de la arquitectura propuesta, de esta forma el servicio queda abierto a posibles mejoras, modificaciones y nuevas aplicaciones que complementen u optimicen el proceso de pago.

Para realizar una evaluación cualitativa se realizaron pruebas de estrés sobre el Servicio Web del AC que se constituye en el módulo central de la arquitectura. La descripción detallada de estas pruebas se presenta en el Anexo B. Los resultados fueron los siguientes:

El valor máximo de consumo de memoria para 75 clientes fue de 102 Mb, para 100 clientes fue de 140, y para 125 clientes fue de 183 Mb, en un equipo con procesador Pentium Core Duo de 1.86GHz y 1Gb de memoria RAM. Por lo cual se puede deducir que para más de 125 clientes simultáneos el sistema comienza a congestionarse, claro que en un punto de creación de cuentas real hay un mayor intervalo de tiempo entre solicitudes de creación de cuenta haciendo que la carga sea menor que en la prueba de estrés.

4.5. Análisis de Resultados

El proceso de validación permitió determinar que la arquitectura de facturación y pago cumple con los servicios y las funcionalidades para las cuales fue diseñado y con los atributos o características de calidad definidas.

A continuación se presenta un análisis de los aspectos más relevantes relacionados con la arquitectura.

Muchas de las características de la arquitectura dependen en gran medida de las tecnologías seleccionadas. Los módulos centrales de la arquitectura de facturación y pago se basan en dos tecnologías, los Servicios Web y LDAP. La primera para el desarrollo de toda la lógica del negocio del modulo Administrador de Cuentas y para facilitar su interacción con los módulos de Creación de Cuentas y Punto de Venta a través de la implementación de el cliente del Servicio Web en ellos. LDAP se constituyó en la base para el almacenamiento de la información en el modulo Administrador de Usuarios.

Los Servicios Web facilitan la implementación de esquemas básicos de seguridad como los firewalls ya que están apoyados sobre el protocolo HTTP. Por otro lado, como se pudo observar en las pruebas de eficiencia la carga por procesamiento y el consumo de memoria son bajos, lo que le brinda eficiencia a la plataforma.

El manejo de la información a través de LDAP le da rapidez al sistema ya que esta tecnología permite realizar lecturas muy rápidas de los registros, la interfaz hacia esta base de datos es fácil de implementar, ya que se monta sobre TCP/IP y permiten la ejecución de esquemas de seguridad basados en SSL.

La tecnología RFID usada en el dispositivo móvil permite la implementación del esquema de pago por proximidad y como consecuencia del uso de estándares en la comunicación se facilita la interoperabilidad y la flexibilidad en el momento de adoptar tecnologías más modernas como NFC.

La seguridad es uno de los aspectos críticos en la arquitectura de facturación y pago debido al tipo de servicio que presta en donde se encuentra involucrado dinero y esto hace que para los usuarios y las entidades participantes sea de mucha importancia.

La seguridad de un sistema depende tanto de factores técnicos como de las políticas que se implementen tanto en las entidades participantes como por los usuarios mismos. A nivel técnico las pruebas demostraron que la arquitectura es segura adicionándole un elemento que no se había considerado inicialmente como lo es el firewall en los módulos de Administrador de Cuentas y Administrador de Usuarios, esto se puede ver en el Anexo B. Este firewall eleva la seguridad en el

sistema pero no lo hace invulnerable, ya que técnicas como el cifrado protegen la información pero pueden ser violadas por personas expertas.

Otro punto bastante importante son las entidades certificadoras, las cuales deben cumplir con todos los requerimientos que para ellas se exigen [80] y tener un nivel de aceptación tal que todas las partes que intervienen en el proceso confíen en ellas.

A nivel tecnológico el sistema se diseñó con un alto porcentaje de seguridad, pero aun así en las pruebas se detectaron posibles vulnerabilidades del sistema que podían ocasionar suplantación de alguna de las partes, denegación del servicio o alteración del funcionamiento de algunos de los servidores, por esta razón se implementaron medidas adicionales como firewalls y VPN, quedando el sistema final como se muestra en la Figura 32.

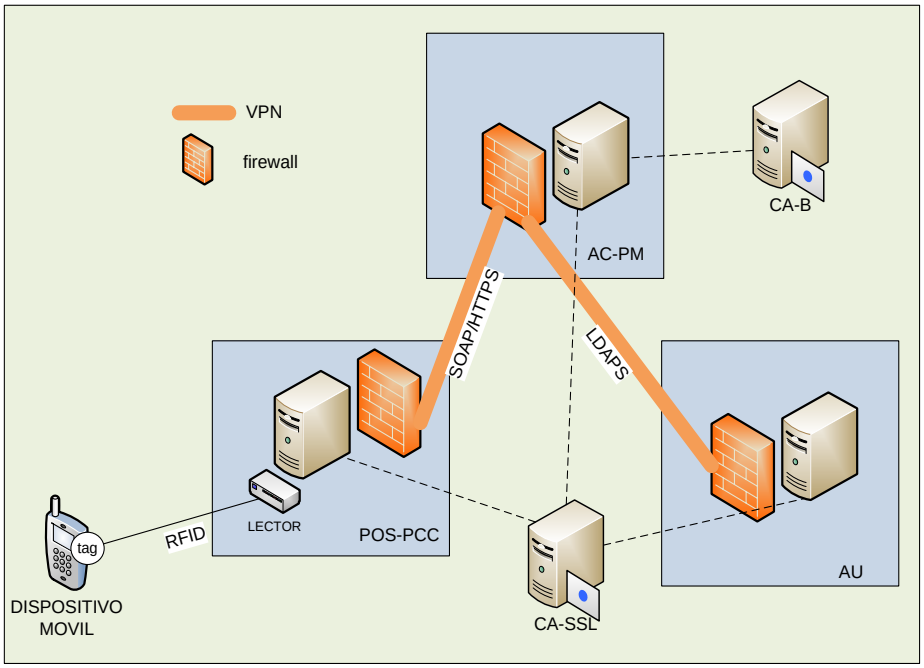


Figura 32. Esquema final de seguridad

A pesar de los esquemas de seguridad implementados, si no existen políticas de protección en las entidades participantes, como los usuarios, los vendedores, los administradores del servicio, entre otros, el sistema podrá fácilmente ser vulnerado.

A continuación se listan algunas normas de seguridad que deberían tener los usuarios y administradores del sistema para garantizar unos niveles adecuados de seguridad. Para la definición de las políticas se siguió el esquema planteado en la tesis de pregrado de la universidad del Cauca titulado: “Criterios para establecer políticas de seguridad de la información y plan de contingencia, caso de estudio el centro de datos de la universidad del Cauca” [81].

- Políticas de seguridad para los administradores de la red y los servicios
    - Monitorear el funcionamiento y rendimiento del servicio de pago, y mantener un registro e historial de los resultados.

- Atender fallas en el servicio a tiempo y solucionarlas lo antes posible.
- Revisar periódicamente las aplicaciones y servicios para plantear posibles mejoras en los mismos.
- En caso de presentarse una falla debido a la instalación de una nueva versión de la aplicación, es obligación del Administrador cambiarla por la versión inmediatamente anterior que funcionaba correctamente.
- A los archivos de configuración de cada Servidor, solo se puede acceder en modo Administrador.
- Mantener una copia de seguridad de las aplicaciones y archivos de configuración en un lugar que solo pueda ser accedido por el administrador.
- El Administrador del Servidor del AU es la única persona que puede acceder a los datos de los usuarios, y debe mantener una copia de los mismos donde solo él tenga acceso.
- El historial de eventos solo puede ser accedido por el Administrador encargado de la seguridad en el servicio.
- No divulgar información confidencial y que comprometa la seguridad del servicio a personas no autorizadas.
- Garantizar la disponibilidad de los datos que puedan requerir tanto los compradores, como los vendedores.
- Velar por la integridad y confidencialidad de los datos, aún cuando estos ya no sean necesarios.
- Los equipos de los servidores se deben encontrar en un lugar seguro y de acceso restringido.
- En caso de necesitarse el acceso de equipo técnico o personal extraño a los servidores, se hará en presencia del administrador o administradores del servidor.
- Los Administradores de cada servidor son responsables por las aplicaciones que se encuentren en dicho equipo.
- Es responsabilidad del Administrador de cada servidor mantener la confidencialidad y robustez de su contraseña de root.
- Mantener una lista actualizada de los clientes y vendedores del sistema.

- Políticas de seguridad para los creadores de cuentas

  - El Creador de Cuentas es el responsable de las aplicaciones e información del equipo PCC.
  - El creador de cuentas es el único que tiene acceso físico al equipo PCC.
  - Al equipo PCC solo se podrá acceder en modo Administrador.
  - Es responsabilidad del Creador de Cuentas mantener la confidencialidad y robustez de su contraseña de administrador.
  - No divulgar información confidencial y que comprometa la seguridad del servicio a personas no autorizadas.
  - Comprobar la veracidad de los datos de los usuarios en el momento de crear la cuenta, solicitando documentos de identidad.
  - Garantizar que todos los datos requeridos para la creación de cuentas sean ingresados.
  - Informar a tiempo sobre fallas en la aplicación del PCC a los administradores del sistema.

- Mantener la línea telefónica de desactivación de cuentas desocupada, para atender solicitudes de eliminación de usuarios a tiempo.

- Políticas de seguridad para los vendedores

  - Velar por la seguridad física del equipo POS.
  - Al equipo POS solo se podrá acceder en modo Administrador
  - Mantener la confidencialidad y robustez de su contraseña de Administrador.
  - Revisar el estado y funcionamiento del terminal de pago periódicamente para garantizar la disponibilidad del servicio.
  - Informar a tiempo sobre fallas en la aplicación de POS a los administradores del sistema.
  - Garantizar que en el momento del pago solo tenga acceso al lector el comprador.
  - En caso de disponer de lector de huella digital, monitorear el proceso de autenticación de usuario.
  - Llevar un registro fotográfico de los compradores.

- Políticas de seguridad para los compradores

  - El servicio de facturación y pago solo se brindará a los usuarios registrados en el sistema SeUS.
  - Verificar los datos suministrados para la creación de la cuenta.
  - Una vez recibe la etiqueta, la integridad de la misma es responsabilidad exclusiva del cliente.
  - El usuario debe llamar inmediatamente en caso de robo o pérdida de su etiqueta RFID, para deshabilitar la cuenta de SeUS.
  - Aceptar como comprobante de pago los medios digitales utilizados en SeUS, como SMS y facturas al correo electrónico.
  - Informar sobre cambio de dirección electrónica al Creador de Cuentas.
  - Informar sobre pérdida o cambio de teléfono celular al creador de cuentas.

4.6. Recomendaciones para la Implantación en el Entorno Colombiano

El uso intensivo y el fortalecimiento de los canales de pago electrónicos dependen tanto de factores de oferta como de factores de demanda [79]. Por el lado de la oferta, aspectos como la regulación, el tipo de productos financieros que se ofrecen, la plataforma tecnológica y los costos son fundamentales para profundizar el uso de medios de pago basados en nuevas tecnologías. Por el lado de la demanda, el nivel de ingreso, el nivel educativo y el grado de bancarización son factores cruciales para incrementar el uso de esos medios de pago. Al ser la plataforma de facturación y pago un medio de pago electrónico también se ve enmarcada dentro de estos aspectos y por tanto el análisis de su implantación en el entorno colombiano se hará desde varios de estos puntos de vista: legales, financieros, técnicos y sociales.

4.6.1. Aspectos Legales

El 18 de agosto de 1999 fue expedida en Colombia la Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones [82]. Este tipo de leyes hacen de Colombia un país pionero en Latinoamérica en legislación de comercio electrónico y se brinda un grado de seguridad a los colombianos que desean comerciar por Internet, además permite la aparición de nuevas tecnologías asociadas y facilita su implantación en el entorno regional.

La ley 527 de 1999 surge del acercamiento con los organismos internacionales interesados en el tema y de los debates e investigaciones realizadas por una comisión designada que incluía representantes tanto de organismos públicos como privados, quienes decidieron tomar como base para la legislación colombiana la ley modelo propuesta por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) [83].

La ley de comercio electrónico colombiana está regida por 5 principios que regulan la materia, estos son [84]:

- Internacionalidad de la ley. La norma debe ser interpretada teniendo en cuenta su carácter internacional y se debe velar porque su interpretación sea uniforme a nivel mundial.
- Autonomía de la voluntad. La ley reconoce la libertad contractual de las personas para regular sus propias relaciones.
- Equivalente funcional. Se refiere a la posibilidad de trasladar la funcionalidad del papel usado en el comercio tradicional, a elementos electrónicos y que estos medios también ofrezcan seguridad y confianza a las transacciones.
- Neutralidad. Pretende que las funcionalidades de la ley no se vinculen con ninguna tecnología en especial.
- Flexibilidad. La ley no regula todos los detalles del comercio electrónico, se adapta a los planteamientos jurídicos existentes.

El mecanismo de seguridad avalado por la Ley está compuesto por:

- La firma digital (digital signature)
- Las entidades de certificación (Certification Authority – CA)
- Los certificados digitales (certificate)
- Los repositorios

Con el fin de facilitar la implantación de la plataforma de facturación y pago en el contexto colombiano, su diseño en cuanto a la seguridad se basó en la ley mencionada, esto se ve reflejado en el hecho de que se usaron dos entidades de certificación CA-SSL y CA-B para la generación de las claves necesarias para el cifrado de la información y para que a través de los certificados digitales se permitiera la autenticación de cada una de las partes que intervienen en el proceso de facturación y pago, además de permitir la firma digital de la factura de pago enviada al usuario.

Debido a que la implementación del piloto se hizo en un ambiente de prueba las entidades de certificación que se usaron fueron propias, pero para una implantación real de la plataforma, estas autoridades deben ser entidades avaladas en el contexto nacional o internacional.

En Colombia, las entidades de certificación son aquellas personas jurídicas y privadas, incluidas las cámaras de comercio que poseen el hardware y software necesarios para la generación para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación y archivo de documentos soportados en mensajes de datos.

La entidad certificadora brinda la tecnología necesaria para generar las claves, desarrolla los procedimientos requeridos para la identificación de los solicitantes, administra el proceso de emisión, verificación y revocación, controla el funcionamiento y desarrolla nuevas tecnologías para incrementar la confiabilidad y seguridad de las transacciones.

Estas entidades son vigiladas por la Superintendencia de Industria y Comercio en lo referente a:

- Acceso al mercado y salida del mismo
- Cumplimiento de todos los requisitos de seguridad en el ejercicio de sus funciones
- Tarifas que cobran por sus servicios
- Expedición de firmas digitales, las cuales pueden ser solicitadas por personas naturales o jurídicas.

La ley de Comercio Electrónico sancionada en Colombia dispuso que un certificado expedido por una entidad certificadora, además de estar firmado digitalmente por dicha entidad, debe contener como mínimo los siguientes requisitos:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

En Colombia, existe una entidad certificadora denominada Certicámara S.A [80], la cual es una empresa filial de las Cámaras de Comercio y Confecámaras, fue creada en el año de 2001 y es la única entidad de certificación digital abierta en el país, autorizada y vigilada por la Superintendencia de Industria y Comercio. Certicamara es el tercero de confianza que garantiza la seguridad jurídica y tecnológica a las transacciones, comunicaciones, aplicaciones y en general a todo proceso de administración de la información digital.

Certicamara cumple con los más altos estándares internacionales exigidos por el *American Institute of Certified Public Accountants* (AICPA) y el *Canadian Institute of Chartered Accountants* (CISA), es auditada por la firma internacional Deloitte y obtuvo el sello WEB TRUST que los califica como una entidad de certificación digital de clase mundial, así como el reconocimiento de Microsoft a sus productos y servicios a nivel mundial.

A nivel internacional existen una gran cantidad de Autoridades de Certificación entre las cuales se destacan:

- VeriSign Inc. [85]: proporciona infraestructura digital que posibilita y protege cada día miles de millones de interacciones en las redes de datos y voz de todo el mundo. Día tras día procesa unos 31.000 millones de interacciones en Internet y hace posible la realización de más de 100 millones de llamadas telefónicas. Ofrece soluciones que ayudan a las empresas a enviar campañas de marketing integradas y contenidos móviles en los tres tipos de pantallas: PC, teléfonos móviles y televisores. Las soluciones Verisign ayudan a las organizaciones a ofrecer servicios emergentes como operaciones bancarias a través de móviles, voz sobre IP (VoIP) y vídeo sobre banda ancha. Proporciona soluciones de seguridad de varios niveles que protegen los clientes, la marca, el sitio Web y las redes de cada organización. Los certificados digitales protegen a más de 750.000 servidores Web.
- GlobalSign [86]: es una autoridad de certificación y proveedora de SSL, bien establecida y con gran credibilidad. Es líder en servicios de confianza y expedición de certificados desde 1996. Los certificados son reconocidos por los principales navegadores web, servidores web, clientes de correo electrónico, aplicaciones de Internet y dispositivos que requieren certificados SSL. Inversores, como Vodafone, han hecho posible que esta empresa se convierta en un experto en el suministro de certificados de confianza y seguros de tecnologías para dispositivos móviles y teléfonos celulares.
- Digital Signature Trust co[87]: DST fue la primera autoridad de certificación licenciada en los Estados Unidos, provee servicios de certificados digitales basados en PKI y soluciones de comercio electrónico para clientes comerciales y del gobierno. DST brinda confianza que permite a las organizaciones obtener todos los beneficios del comercio electroncito.

Respecto al formato de la factura digital, el decreto 1929 sugiere el mismo utilizado en forma impresa, que fue reglamentado en el artículo 617 del Estatuto tributario donde se especifican los siguientes requisitos para una factura de venta [88]:

a. Estar denominada expresamente como factura de venta
b. Apellidos y nombre o razón y NIT del vendedor o de quien presta el servicio
c. Subrogado. Ley 788/2002, Art. 64. Apellidos y nombre o razón social y NIT del adquiriente de los bienes o servicios, junto con la discriminación del IVA pagado
d. Llevar un número que corresponda a un sistema de numeración consecutiva de facturas de venta
e. Fecha de su expedición
f. Descripción específica o genérica de los artículos vendidos o servicios prestados
g. Valor total de la operación
h. El nombre o razón social y el NIT del impresor de la factura
i. Indicar la calidad de retenedor del impuesto sobre las ventas

En lo referente al contenido de la factura electrónica aparecen dos valores nuevos en comparación con la facturación tradicional: clave del contenido técnico de control y el contenido técnico de control. El primero es un certificado con una clave, que el interesado solicita a la DIAN y permite diferenciar a cada establecimiento o vendedor; el segundo es un valor alfanumérico obtenido a partir de la aplicación de un procedimiento que utiliza algunos datos de la factura y la clave de contenido técnico suministrada por la DIAN, y deberá ser incluido como un campo más dentro de la factura generada electrónicamente, siendo un valor único para cada una de ellas. El proceso de

generación del contenido técnico de control se explica mejor en el anexo 001 de la resolución 14465 de la DIAN [89].

La factura digital de la compra generada por la plataforma de facturación y pago contiene todos estos campos, y por tanto cumple a cabalidad con la ley y puede ser aceptada en el contexto financiero colombiano.

Como puede observarse, la arquitectura de facturación y pago se ajusta a la ley colombiana ya que la seguridad está basada en entidades de certificación demostrando la validez de la ley y convirtiéndose en un ejemplo de su implementación y se manejan facturas digitales las cuales son aceptadas legalmente como se mostró anteriormente.

4.6.2. Aspectos Financieros

La plataforma de facturación y pago propuesta está basada en cuentas bancarias, de las cuales en últimas será de las que se haga el debito correspondiente para hacer efectivo el pago. El acceso de las personas tanto a un dispositivo móvil con la tecnología RFID implantada como a una cuenta bancaria se constituyen en uno de los principales requisitos para que la plataforma pueda ser implantada en el entorno colombiano.

En el país el acceso a los servicios financieros, entre los que se consideran las cuentas de ahorro y cuentas corrientes, tarjetas débito y crédito, otros servicios de pago, préstamos de consumo, micro créditos y remesas, es bajo, pero presenta una tendencia al alza. De acuerdo con las cifras a marzo de este año, más de 15.6 millones de colombianos mayores de edad tienen acceso al menos a un producto financiero, lo que representa un nivel de bancarización de 55.5% de la población adulta. Este resultado representa un aumento de más de 1,3 millones de personas frente a marzo de 2007, y un incremento de más de 166 mil personas frente a diciembre del año anterior [90].

La cuenta de ahorro es el producto financiero con mayor grado de penetración en el país. Más de 15 millones de personas adultas tienen una cuenta, lo que representa el 53.35% de la población mayor de 18 años. El incremento de personas adultas con este producto en el último año fue 10%. El número de personas menores de edad con tarjeta de identidad que tienen una cuenta de ahorro subió en más de 373 mil en ese lapso, lo que representa un avance significativo de la cultura de ahorro y del aprendizaje en el uso de los instrumentos financieros tradicionales desde edades tempranas [90].

Con el fin de mejorar el acceso a los servicios financieros el gobierno colombiano ha lanzado el proyecto de “Banca de Oportunidades” [91] el cual es una estrategia de política de largo plazo del Gobierno Nacional, dirigida a lograr el acceso a servicios financieros para la población de bajos ingresos con el fin de reducir la pobreza, promover la igualdad social y estimular el desarrollo económico colombiano. La Banca de las Oportunidades tiene como objetivo crear las condiciones necesarias para facilitar el acceso a servicios de crédito y otros servicios financieros como ahorro, transferencias, pagos, giros, remesas y seguros, a las poblaciones que no han tenido acceso a los mismos.

La mejora en el acceso a servicios financieros también abarca el uso de medios de pago diferentes al efectivo, por una proporción cada vez más importante de la población. Las nuevas tecnologías ofrecen canales electrónicos como el Internet, las tarjetas inteligentes y los teléfonos móviles que

pueden contribuir de manera muy positiva a mejorar el acceso a los servicios financieros y en particular a medios de pago más eficientes [79].

El uso de teléfonos móviles se ha extendido enormemente en los últimos años hasta el punto de llegar a ser la primera tecnología de comunicaciones con mayor número de usuarios en países en desarrollo que en países desarrollados. Las tecnologías móviles han supuesto un salto de etapa evitando el paso por la estructura de telefonía tradicional en muchos países en desarrollo, y el uso de dispositivos móviles para servicios financieros puede convertirse en otro salto de etapa al facilitar el acceso a servicios financieros a población no bancarizada, con una tecnología que resulta familiar y está suficientemente extendida [92].

Como conclusión se puede observar que a pesar de que el nivel de bancarización en Colombia es muy reducido en los sectores de menos ingresos, existe una preocupación muy grande en el gobierno por ampliar la cobertura, esto unido al hecho de que la telefonía móvil ha tenido una penetración muy grande en el país, presenta un panorama interesante para la implementación de tecnologías basadas en dispositivos móviles para acceder a servicios financieros, entre los cuales podría tener una amplia cabida la arquitectura de facturación y pago propuesta.

Por otro lado es importante tener en cuenta que los bancos que acepten prestar el servicio a sus usuarios para poder acceder a la plataforma de facturación y pago, deben poder brindar la opción de habilitar las cuentas para permitir pagos móviles. A pesar de que este servicio aun es muy incipiente en nuestro país se puede observar que casi todas las entidades financieras están abriendo su portafolio de servicios hacia nuevas tecnologías que faciliten a los usuarios la realización de transacciones financieras [79].

4.6.3. Aspectos Técnicos

Colombia cuenta actualmente con las condiciones de infraestructura necesarias para la implementación de novedosos servicios financieros basados en tecnologías ubicuas, como la arquitectura de facturación y pago propuesta:

- Alta penetración de la telefonía móvil
- Redes de banda ancha para el acceso a Internet
- Acceso a Internet desde dispositivos móviles

El Ministerio de Comunicaciones en su último informe Trimestral de Telefonía Móvil TMC y PCS [93], indicó que en el trimestre julio a septiembre del año 2008 existían 39.048.988 abonados de telefonía móvil en servicio. El número de abonados para el año 2007 fue 33.941.118, en el año 2006 fue de 29.762.118 y en el 2005 fue de 21.849.993, lo cual representa un incremento de 36% entre los años 2005 y 2006 y del 14% entre 2006 y 2007 y del 15% entre 2007 y 2008.

Respecto a Internet, los suscriptores del servicio de acceso a Internet aumentaron un 11% en el tercer trimestre de 2008, llegando a 1.969.023. Aquéllos que utilizan accesos dedicados aumentaron un 12,2% alcanzando 1.777.881, mientras que los que utilizan accesos conmutados aumentaron un 0,6% llegando a 191.142, esto indica una preferencia de los usuarios por los accesos dedicados acogiendo de esta manera tecnologías que permiten utilizar un número mayor de aplicaciones y obtener mejores desempeños.

En el primer semestre de este año, los operadores móviles facturaron más de 47 mil millones de pesos por los servicios de acceso a Internet. Los suscriptores enviaron 1.183 millones mensajes de texto. Según los datos reportados por Comcel, Movistar, Tigo y Avantel a la CRT [94], durante el primer semestre del año 5,3 millones de usuarios celulares accedieron a Internet desde sus teléfonos, lo que equivale al 14,8 por ciento de los 35,8 millones de abonados móviles que existen en el país.

Esta cifra contrasta con el informe de marzo pasado en el que el número de usuarios móviles que accedían a la Red llegó a 3,4 millones, el 10,2 por ciento del total. Igualmente, el tráfico de Internet generado por los abonados móviles del país creció 83,7 por ciento entre el primero y el segundo trimestre del año, lo cual significa que están usando ese servicio mucho más que antes [94].

Además del interés que demuestran los colombianos por la telefonía celular y por el acceso a internet a través de ellos, existe una tendencia entre los usuarios en adquirir equipos con mejores prestaciones, lo cual hace más viable la adaptación de etiquetas RFID a los dispositivos móviles o la adquisición de teléfonos con tecnología NFC integrada. Esto se evidencia en la Figura 33. En donde se muestran los resultados de una encuesta realizada por CINTEL en el 2005 [95].

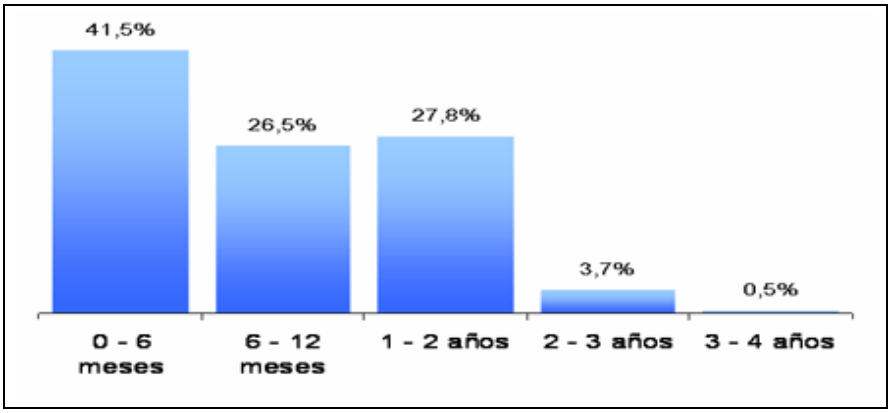


Figura 33. Tiempo desde la última vez que cambiaron o adquirieron celular

Todas estas cifras muestran que el esfuerzo que se tendría que hacer a nivel tecnológico en Colombia para la adopción de una plataforma de facturación y pago como la propuesta es mínimo, ya que como se mostró todas las condiciones están dadas.

Teniendo en cuenta las recomendaciones mencionadas y la plataforma de facturación y pago propuesta, para la creación de un proveedor de pago debería tener en cuenta los siguientes aspectos:

- Cumplir con la legislación colombiana para el uso de certificados digitales, firmas digitales y facturas digitales.
- Obtener los certificados digitales de alguna institución avalada nacionalmente, como Certicamara, o internacionalmente como Verisign.

- Establecer una relación con un banco, para que permita realizar pagos móviles a través de las cuentas de sus usuarios.
- Implementar la interfaz al banco de tal manera que cumpla con los requerimientos de seguridad exigidos por él, en cuanto a autoridades de certificación y protocolos de comunicación.
- Permitir el pago desde dispositivos móviles de todos los tipos, los de gama baja y media con el uso de etiquetas RFID y los de gama alta que tengan inmersa la tecnología NFC.
- Realizar acuerdos de servicio con los operadores de telefonía celular que permitan el envío de los mensajes de texto a través de sus redes a los usuarios.

4.6.4. Aspectos Sociales

A pesar de la gran penetración de la telefonía móvil y la tendencia al alza en las cifras mostradas Colombia aun se encuentra atrasada con respecto a la penetración de las TIC en los sectores menos favorecidos. Pero el gobierno es consciente de este problema y dentro de su plan de desarrollo al 2010 ha incluido planes para lograr el cierre de la brecha digital entre los cuales se pueden mencionar [96]:

- Adaptar el marco normativo e institucional a la convergencia tecnológica y promover la competencia
- Preparar al sector para la globalización de servicios
- Garantizar niveles apropiados de acceso y servicio universal
- Lograr coberturas de servicios de voz y datos (Internet), acordes con las metas de desarrollo económico del país

Los ejes del plan de gobierno son:

1. Todos los colombianos conectados e informados
2. Consolidación y modernización institucional que genere un sector estratégico para el país
3. Desarrollo y competitividad de la industria de telecomunicaciones e informática
4. Política para la televisión pública y la radio

Por otro lado, estudios realizados muestran que la alta penetración de la telefonía móvil, la cual ha sido bastante pronunciada en los sectores de más bajos ingresos, es muy apreciada por ellos como una herramienta para fortalecer los lazos sociales y tener mayor seguridad personal, y está empezando a ser considerada útil para mejorar los negocios y las oportunidades de trabajo, en mayor grado en los mercados laborales informales [97].

Dado el limitado acceso a los tradicionales servicios de telefonía fija, los pobres atribuyen una significativa mejoría en su calidad de vida al acceso a la telefonía móvil. El considerable nivel de gasto en aparatos y servicios de telefonía móvil entre esta población de bajos recursos también es consistente con los numerosos beneficios percibidos por los usuarios.

Los resultados del estudio [97] demuestran que existe un amplio campo para iniciativas de beneficio general que aumenten el tráfico total y creen nuevas oportunidades comerciales para los operadores y terceros, que van desde simples servicios de información a servicios de transacciones más complejas.

Se requerirá un esfuerzo concertado entre los actores del mercado, los cuales pueden ser tan diversos como operadores de telefonía, proveedores de servicios, empresas financieras, desarrolladores, entre otros, para aprovechar las oportunidades creadas por el uso generalizado de la telefonía móvil y de internet y los planes del gobierno, que permiten la adopción de servicios novedosos como el mostrado en la plataforma de facturación y pago propuesta. Y en la medida en que estos usuarios se sientan seguros con las nuevas tendencias tecnológicas, las oportunidades de servicios móviles continuarán aumentando. Muchas de las aplicaciones que podrían beneficiar a todos los sectores de la población, tales como servicios bancarios y gubernamentales (m-banking, m-government, m-payment) son aún incipientes en la región, pero se presenta un buen panorama para su desarrollo.

Capítulo 5

CONCLUSIONES, APORTES Y TRABAJOS FUTUROS

5.1. Conclusiones

A continuación, se presentan las conclusiones más relevantes del desarrollo de la Plataforma de Facturación y Pago para Ambientes Ubicuos.

5.1.1. Generales

- La visión de Mark Weiser acerca de la computación ubicua cada vez está más cerca, a nivel de infraestructura y de software se cuenta con las herramientas necesarias para empezar a desarrollar esa visión, y en Colombia, a pesar de no ser un país con los más altos niveles de desarrollo tecnológico, es factible el desarrollo de servicios en este campo y la arquitectura propuesta en este trabajo es una muestra de ello.
- La plataforma servirá de base para el desarrollo y prueba de otro tipo de servicios, potenciando de esta manera la investigación en este campo, aun incipiente en nuestro país.
- La gran penetración de la telefonía celular, con especial énfasis en los estratos más bajos, brinda un buen panorama para el desarrollo de servicios que se soporten en los dispositivos móviles. El acceso a este tipo de servicios de los sectores menos favorecidos será un aporte al programa de cierre de la brecha digital que está promoviendo el gobierno.
- La plataforma de facturación y pago se adapta e implementa la ley colombiana de comercio electrónico, ya que tiene su base en entidades de certificación y firmas digitales, mecanismos que se usaron en la plataforma para implementar los esquemas de seguridad.
- Colombia cuenta con la infraestructura necesaria para la implementación de servicios novedosos basados en computación móvil y/o ubicua, se tiene una gran cobertura de telefonía celular, proveedores de servicios de banda ancha, los cuales cada vez son más apetecidos por los usuarios, operadores de telecomunicaciones que están actualizando su tecnología con redes de próxima generación, como el caso de Emcali en la ciudad de Cali, lo cual indica que a nivel tecnológico la implementación de la arquitectura propuesta es factible.

5.1.2. Técnicas

- La plataforma de Facturación y Pago para ambientes ubicuos brinda seguridad a los usuarios y a las entidades participantes a través del uso de certificados digitales que permiten autenticar a los participantes en el proceso, y validar la factura digital a través de una firma digital.
- El uso de claves tanto públicas como privadas, generadas por las entidades certificadoras, permite cifrar la información que se transmite entre los módulos durante todo el proceso de facturación y pago, esta técnica permite salvaguardar la información de posibles intrusos.

- A pesar de todas las medidas de seguridad implementadas en la arquitectura no se puede decir que ella sea inmune a estos inconvenientes en su totalidad, pueden existir problemas de seguridad por las malas prácticas de las personas involucradas en el proceso, por la ausencia de políticas de seguridad adecuadas o por el no cumplimiento de las mismas.
- Las tecnologías y herramientas empleadas en la implementación de la arquitectura, como los Servicios Web, LDAP, garantizan la interoperabilidad del sistema, ya que ellas son abiertas y no dependen de la infraestructura sobre la cual se montan. Además, le dan robustez al sistema ya que permiten manejar un número amplio de clientes accediendo al servicio.
- Debido a que los dispositivos móviles que integran la tecnología NFC aun no están muy difundidos en el país, la arquitectura propuesta permite la utilización de etiquetas RFID que pueden adherirse al dispositivo, facilitando su implantación en el entorno.

5.1.3. Metodológicas

- Abordar el diseño de la solución de facturación y pago a través de una arquitectura de software, permitió un proceso de desarrollo más ordenado y eficiente, ya que se ataca el problema desde un nivel de abstracción alto, el cual se va bajando a través de los módulos permitiendo enfocarse en problemas más simples y establecer relaciones entre ellos para llevar a cabo la función principal. Este mecanismo también permite desarrollar las pruebas más fácilmente.
- El realizar las pruebas de la arquitectura a través de un piloto de prueba como SeUS permitió demostrar que a nivel técnico la implementación de la arquitectura es totalmente factible, que en Colombia se cuenta con la tecnología y los conocimientos necesarios para su implantación. Las pruebas también demostraron que los tiempos de respuesta a las solicitudes de servicios son aceptables y cumplen con las normas que para tal fin existen en el país.
- El piloto de prueba permitió también demostrar que los esquemas de seguridad planteados para la arquitectura son los adecuados para el tipo de servicio propuesto, ya que aseguran en gran medida la confidencialidad de la información, la autenticidad de los participantes, la privacidad de los datos de los usuarios; pero a su vez no carga al sistema con tanto procesamiento extra que impida la ubicuidad del sistema.

5.2. Aportes

5.2.1. Técnicos

- A nivel investigativo, la plataforma desarrollada sirvió para elaborar una base de conocimiento alrededor de la computación ubicua, haciendo un especial énfasis en los aspectos relacionados con la seguridad asociada a servicios de facturación y pago, permitiendo de esta manera acortar la distancia tecnológica que nos separa de los países desarrollados.
- La plataforma de facturación y pago propuesta es una de los primeros sistemas que implementa la ley de comercio electrónico colombiana y hace uso de la especificación de la DIAN en cuanto a facturas digitales. Esto la convierte en un modelo bastante interesante para demostrar la aplicabilidad de este tipo de legislación en nuestro país.
- A pesar de que la computación ubicua es bastante reciente y apenas se está expandiendo en los países desarrollados, la plataforma propuesta permite demostrar, dadas sus características, que este tipo de tecnologías son implementables en el entorno colombiano, ya que debido a la utilización de etiquetas RFID se puede acceder al servicio usando dispositivos

de gama media y baja, comunes en Colombia, aunque debido al uso del estándar 14443B el sistema también puede adaptarse s teléfonos móviles de nueva generación que cuenten con NFC.

- El sistema de pago propuesto en la plataforma es espontaneo y de fácil uso, ya que no requiere de claves ni de mensajes por parte del usuario para confirmar la transacción, sin que esto degrade los niveles de seguridad. Esto lo hace diferente a la mayoría de los sistemas de pago existentes en el país.
- La implementación de la plataforma propuesta en un entorno real traerá beneficios a distintos actores: a los usuarios quienes tendrán la posibilidad de acceder a aplicaciones que le facilitarán algunas de sus tareas diarias, como el pago de servicios; a las empresas proveedoras de servicios, ya que la incursión en este tipo de tecnologías permitirá la potenciación de sus redes y equipos, y aceleraran los procesos de retorno de inversión, a las entidades financieras quienes podrán dar una valor añadido a sus productos financieros al permitir el pago de servicios ubicuos a través de ellos, a los operadores quienes aumentaran el trafico en sus redes, entre otros.
- Para la implementación del piloto de prueba se realizaron aplicaciones y configuraron herramientas, que se convierten en un aporte a la comunidad académica de la Facultad al ser de utilidad en otro tipo de aplicaciones, diferentes a un sistema de pago. Entre ellos cabe mencionar: transferencia segura entre una etiqueta y un lector RFID, empleando el estándar14443b, transferencia de datos desde Java a un dispositivo por medio del puerto USB, empleando JNI, conexión de forma segura a un directorio LDAP desde un Servicio Web Java empleando JNDI, configuración de herramientas de seguridad como firewalls y VPN entre servidores, despliegue de un Servicio Web Seguro basado en WS-Security.

5.2.2. Publicaciones

PONENCIA

Ponencia titulada “Propuesta de Arquitectura para Facturación y Pago por Proximidad de Servicios Ubicuos en el Contexto Colombiano” presentado en el I2COMM 2008, evento que se llevó a cabo los día 21 y 22 de febrero en la ciudad de Cartagena, y publicado en las memorias de dicho evento.

ARTICULOS

Artículo titulado “Propuesta de Arquitectura para Facturación y Pago por Proximidad de Servicios Ubicuos en el Contexto Colombiano” publicado en la Revista S&T, Sistemas y Telemática Nº 11 de la Universidad ICESI. ISSN 1692-5238.

Artículo titulado “Plataforma para Servicios de Facturación y Pago en Ambientes Ubicuos” presentado para publicación en la revista “Ingeniería y Universidad” editada por la Facultad de Ingeniería de la Pontificia Universidad Javeriana. ISSN 0123-2126.

5.2.3. Consolidación WAP Colombia

El grupo de investigación GIT, al interior del cual se desarrolló esta proyecto, abre otra área de investigación en la cual podrán desarrollarse diversos proyectos asociados a esta temática, brindando nuevas posibilidades a los integrantes del grupo y a los estudiantes tanto de pregrado

como de postgrado que estén interesados en estas nuevas áreas, beneficiando de esta forma tanto a los investigadores quienes incursionarán en nuevos campos de investigación que los colocará a la vanguardia tecnológica, como a los estudiantes quienes se acercaran mas a los avances tecnológicos, lo cual les dará un valor agregado en su preparación para la vida profesional,

5.3. Trabajos Futuros

Este proyecto se constituye en uno de los primeros trabajos relacionados con la Computación Ubicua, desarrollados en el Grupo de Ingeniería Telemática de la Universidad del Cauca GIT, y a partir de él se inicia todo un proceso alrededor de esta temática en donde cabe destacar la propuesta de creación de un Centro de Excelencia en Computación Ubicua, con varias universidades y entidades de la región.

Dentro de esta iniciativa se han planteado varias líneas de acción que se mencionan a continuación:

- Desarrollo de la infraestructura necesaria relacionada con la interacción del usuario con su entorno, conectividad y potencia de cómputo, para poder brindar un servicio personalizado adecuado en términos de funcionalidad de las capacidades del terminal, la prioridad en la entrega de datos, los atributos del usuario y su ubicación geográfica.
- Especificación, análisis y aplicación de los servicios de contexto y comunes que serán utilizados/orquestados por servicios de niveles superiores. Los servicios de contexto permiten ofrecer transparencia, movilidad y sensibilidad al contexto a los usuarios de las aplicaciones. De la misma manera, los servicios comunes ofrecen una serie de servicios compartidos por aplicaciones en diferentes dominios.
- Especificación, análisis e implementación de servicio de dominio que serán utilizados/orquestados para configurar aplicaciones en el dominio de la salud.
- Orquestación de los servicios de contexto, comunes y de dominio en aplicaciones, personalizadas de acuerdo a los perfiles del usuario y la sensibilidad al contexto.

REFERENCIAS

[1] Weiser M. The Computer for the Twenty-First Century. Scientific American, pp. 94-10, September 1991.

[2] Gimeno JM. Computación Ubicua. Capítulo 1. Revista La Flecha. Diciembre 2004. Disponible en: http://www.laflecha.net/articulos/ciencia/computacion_ubicua/

[3] Almenarez, F. "Arquitectura de Seguridad para Entornos de Computación Ubicua Abiertos y Dinámicos". Tesis Doctoral. Universidad Carlos III De Madrid. España. Diciembre 2005

[4] Davies N, Gellersen H. Beyond Prototypes: Challenges in Deploying Ubiquitous Systems. IEEE pervasive computing, 2002.

[5] Boddupalli, P.; Al-Bin-Ali, F.; Davies, N.; Friday, A.; Storz, O.; Wu, M. "Payment support in ubiquitous computing environments". Mobile Computing Systems and Applications, 2003. Proceedings. Fifth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2003), vol., no., pp. 110-120, Octubre 2003.

[6] A. Ranganathan and R.H. Campbell, "Advertising in Pervasive Computing Environment", ACM International Workshop on Mobile Commerce, Atlanta, Georgia, September 28, 2002, pp 10-14.

[7] La evaluación de los sistemas de pago en América Latina. An Economist Intelligence Unit white paper sponsored by Visa International. The Economist Intelligence Unit 2005

[8] Becker K. Emerging Payments Industry Briefing. An Informative Guide to Consumer Payment Behavior. Federal Reserve Bank of Boston. 2007.

[9] Accepting Contactless Payments: A Merchant Guide. A Smart Card Alliance Contactless Payments Council White Paper. 2007

[10] Enabling Secure, Interoperable, and User-friendly Mobile Payments Mobile Payment Forum White Paper. December 2002

[11] Imbus, J. Ausecha M. Arquitectura para pago y facturación de servicios ubicuos. Tesis Universidad del Cauca. 2008.

[12] Paying by Mobile. White paper. Juniper Research. Mobile Payments, Strategies & Markets 2007-2011.

[13] The Big Micropayment opportunity. White paper. Juniper Research. 2004.

[14] Saxena, A.; Lal Das, M.; Gupta, A. "MMPS: a versatile mobile-to-mobile payment system," Mobile Business, 2005. ICMB 2005. International Conference, vol., no., pp. 400-405. Julio 2005.

[15] Srivastava L. Ubiquitous Network Societies: The Case of Radio Frequency Identification. Background Paper. ITU Workshop on Ubiquitous Network Societies. ITU. March 2005.

[16] Ecma International. Near Field Communication [White paper]. Ecma/TC32-TG19/2004/1. 2004

[17] Mobile Payment Forum. Proximity Payment Technology Assessment. Proximity Payment Activity, Version 1.0.0. 2 December 2004

[18] Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure. A Smart Card Alliance Contactless Payments Council White Paper. 2007.

[19] Fleisch E. ITU ubiquitous network societies: their impact on the telecommunication industry background paper. Workshop on Ubiquitous Network Societies. 2005

[20] M.O. Ahmed, S.M.V. Hailes, and A. Seleznyov. The Dangers Of Invisible Computing: Learning To Live With Uncertainty. InUbiconf 2004, Gresham College, London, UK, April 2004.

[21] Chanson, S. Wong, C. Hung, P. Electronic payment systems (EPS). Institutional repository. Hong Kong University of Science and Technology library. Nov-1998
[22] Kadhiwal S, Anwar M. Analysis of mobile payment security measures and different standards. Revista Computer Fraud & Security. Junio 2007.
[23] Gordon A. G. Privacy and Ubiquitous Network Societies [Background Paper]. ITU Workshop on Ubiquitous Network Societies. ITU March 2005.
[24] Servicios Informáticos. Universidad de Navarra. Pamplona. "Nociones sobre Criptografía - Criptografía y firma digital". Diciembre de 2007. Disponible en: http://www.unav.edu/SI/servicios/seguridad/certifica8.html
[25] López, C. "Sistema de Seguridad para Intercambio de Datos en Dispositivos Móviles". Tesis de Maestría, Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional de México. México. Abril 2005.
[26] Miller, S. "Facing the challenge of wireless security". Computer , vol.34, no.7, pp.16-18, Julio 2001.
[27] Caicedo O, Universidad del Cauca. Tesis de Maestría: Plataforma De Comercio Móvil Para El Sector Artesanal Colombiano.
[28] Hardjono, T.; Dondetic L. Security in Wireless LANs and MANs. Artech House Computer Security. 2005
[29] Seema, N.; Lu, C.; Liang, L.R. "Analysis of payment transaction security in mobile commerce". Information Reuse and Integration, 2004. IRI 2004. Proceedings of the 2004 IEEE International Conference, vol., no., pp. 475-480, Noviembre 2004.
[30] Labrou Y., Agre J., Ji L., Molina J., Chen W. Wireless Wallet. Fujitsu Laboratories of America. Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04). 2004.
[31] Gao J., Cai J., Patel K., Shim S. A Wireless Payment System. Computer Engineering, San Jose, USA. Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05). 2005
[32] Boddupalli P., Al-Bin-Ali F., Davies N., Friday A., Storz O. Wu M. Payment Support in Ubiquitous Computing Environments. Proceedings of the Fifth IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2003). 2003
[33] PayPal [online]. Disponible en: https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/mobile/MobileWaysToUse-outside
[34] Mobypay. "Sistema de pago por móvil - Mobypay". Julio 2008. Disponible en: www.mobipay.es
[35] Vilmos A., Karnouskos S. SEMOPS: Design of a New Payment Service. Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03). 2003
[36] Albin S. T., "The Art of Software Architecture: Design Methods and Techniques", John Wiley & Sons. 2003.
[37] Fowler, M. "Patterns of Enterprise Application Architecture". The Addison-Wesley Signature Series. 2004.
[38] Eckerson, Wayne W. "Three Tier Client/Server Architecture: Achieving Scalability, Performance, and Efficiency in Client Server Applications." Open Information Systems 10, 1 1995.
[39] Scaling the N-Tier Architecture. White Paper, Sun Microsystem. Disponible en: www.sun.com/software/whitepapers/wp-ntier/wp-ntier.pdf.
[40] Clements, P. Bachmann, P. Documenting Software Architectures. Addiscon Wesley, Ed. 2002.

[41] Eriksson, H. Penker, M. UML Toolkit. Unified Modelling Language. John Wiley and Sons Ed. 1998.
[42] Monarch Products and Services. RFID Basics Updated Including Gen 2 [White Paper]. May 2006.
[43] R. Moroz Ltd. "Understanding Radio Frequency IDentification (RFID) (Passive RFID)". Noviembre 2004. Disponible en: http://www.rmoroz.com/rfid.html
[44] HID Global. "iCLASS tag datasheet – Tag inteligente adhesivo sin contacto". Marzo 2007. Disponible en: http://www.hidglobal.com/documents/iclass_tag_ds_es.pdf.
[45] International Standards Organization/International Electrotechnical Commission. "Identification cards, Contactless integrated circuit cards, Proximity cards, Part 4: Transmission protocol". ISO/IEC 14443-4:2008. Julio 2008.
[46] Package javax.swing. Disponible en: http://java.sun.com/j2se/1.4.2/docs/api/javax/swing/package-summary.html
[47] iCLASS™ Serial Protocol Interface Version 2.4. Document Number 6090-902, Rev B. HID Global Corporation. 2006.
[48] Liang S. "The Java Native Interface Programmer's Guide and Specification". Addison-Wesley - Sun Microsystems. 1999.
[49] Web Services Security: SOAP Message Security 1.1. (WS-Security 2004). OASIS Standard Specification, 1 February 2006.
[50] Web Services Security: SAML Token Profile 1.1. OASIS Standard, 1 February 2006
[51] Gupta A, Kohlert D. "The Java API for XML-Based Web Services (JAX-WS) 2.1 Maintenance Release". Sun Microsystems, JSR-224. Mayo de 2007.
[52] Glassfish. "Glassfish Community - GlassFish Project – Documentation". 2008. Disponible en: https://glassfish.dev.java.net/javaee5/docs/DocsIndex.html
[53] Core J2EE Patterns - Data Access Object. Disponible en: http://java.sun.com/blueprints/corej2eepatterns/Patterns/DataAccessObject.html
[54] VeriSign. "Centro de información de SSL - Certificados de Seguridad SSL". Julio 2008. Disponible en: http://www.verisign.es/ssl/ssl-information-center/index.html
[55] XCA. "Introduction". Enero de 2007. Disponible en: http://xca.sourceforge.net/xca-1.html
[56] OpenSSL Project. Disponible en: http://www.openssl.org/
[57] Hodges, J.; Morgan, R. "Lightweight Directory Access Protocol (v3): Technical Specification". Internet Engineering Task Force, RFC 3377. Septiembre 2002.
[58] Oracle. "Berkeley DB Reference Guide, Version 4.7.25". Mayo de 2008. Disponible en: http://www.oracle.com/technology/documentation/berkeley-db/db/ref/toc.html
[59] Object XP. "jSMS User's Guide". 2006. Disponible en: http://www.objectxp.com/src/jsms/users_guide.pdf
[60] JavaMail. Sun Developers Network. Disponible en: http://java.sun.com/products/javamail/
[61] Sun Microsystems. "Java Cryptography Architecture API Specification & Reference". Julio 2004. Disponible en: http://java.sun.com/j2se/1.5.0/docs/guide/security/CryptoSpec.html
[62] Sun Microsystems. "Glosario". Sun Microsystems Documentation. Mayo 2008. Disponible en: http://docs.sun.com/app/docs/doc/820-4545/glossary-1?l=es&a=view
[63] Innovision Research & Technology. "Near Field Communication in the real world - Turning the NFC promise into profitable, everyday applications". Agosto 2006. Disponible en: http://www.kstinternational.com/download/paper/200601/IRT_NFC_white_paper_I___FINAL.doc
[64] HTTP over TLS, RFC 2818. Disponible en http://tools.ietf.org/html/rfc2818
[65] SSL/TLS Strong Encryption: An Introduction. The Apache Software Foundation. Disponible en: http://httpd.apache.org/docs/2.0/ssl/ssl_intro.html

[66] Camacho, E. Cardeso, F. Nuñez G. Arquitecturas De Software. Guía De Estudio. Universidad Simon Bolivar. 2004. Venezuela. Disponible en: http://prof.usb.ve/lmendoza/Documentos/PS-6116/Guia%20Arquitectura%20v.2.pdf.

[67] Bosch, J. Design & Use of Software Architectures. Material del curso CECS454, Computer Enginering and Computer Science. California State University.

[68] Metro. "Discover Metro - Metro Web Service Stack Overview". 2007. Disponible en: https://metro.dev.java.net/discover/

[69] Liang S. "The Java Native Interface Programmer's Guide and Specification". Addison-Wesley - Sun Microsystems. 1999.

[70] Debian. "Razones para escoger Debian" Junio 2008. Disponible en: http://www.debian.org/intro/why_debian

[71] DistroWatch. "Las 10 mejores distribuciones - Una revisión de las mejores distribuciones del momento". 2008. Disponible en: http://distrowatch.com/dwres.php?resource=major

[72] Glassfish. "Glassfish Community - GlassFish Project – Documentation". 2008. Disponible en: https://glassfish.dev.java.net/javaee5/docs/DocsIndex.html

[73] Schema for the SOAP/1.1 envelope. W3C (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University).2001. Disponible en: http://schemas.xmlsoap.org/soap/envelope/

[74] Data Access Object (DAO) Code Generator version 2.4.1. TitanicLinux.Net :: DaoGen. Dsiponible en: http://www.titaniclinux.net/daogen

[75] Hodges, J.; Morgan, R. "Lightweight Directory Access Protocol (v3): Technical Specification". Internet Engineering Task Force, RFC 3377. Septiembre 2002.

[76] HID Global. "iCLASS tag datasheet – Tag inteligente adhesivo sin contacto". Marzo 2007. Disponible en: http://www.hidglobal.com/documents/iclass_tag_ds_es.pdf

[77] Losavio de Ordaz, F, Guillen-Drija, C. Conceptual Framework for Architectural Design Based on Quality Aspects. SAPIENS. 2006, vol.7, no.2 p.119-138. Disponible en:<http://www2.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1317-58152006000200009&lng=en&nrm=iso>. ISSN 1317-5815.

[78] Microsoft. "Common Types of Network Attacks". Microsoft TechNet. Disponible en: http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/cnet/cndb_ips_ddui.mspx?mfr=true

[79] Arbeláez, M. Zuluaga, S. Medios de Pago Electrónicos en Colombia: Evolución y Perspectivas. Informe final para comentarios. FEDESARROLLO. Junio de 2006.

[80] Introducción al servicio digital de Certicamara. Disponible en: http://www.certicamara.com. 2007

[81] Guevara, C.; Mera, F. "Criterios para establecer políticas de seguridad de la información y plan de contingencia, caso de estudio el centro de datos de la universidad del cauca". Tesis de Pregrado. Facultad de Ingeniería Electrónica y Telecomunicaciones., Universidad del Cauca, Popayán, Colombia, Marzo 2008.

[82] Poder Público - Rama Legislativa. "Ley 527 de 1999". Diario Oficial No. 43.673. Agosto 1999. Disponible en: http://www.secretariasenado.gov.co/leyes/L0527_99.HTM

[83] Comisión de las Naciones Unidas para el derecho Mercantil. CNUDMI. En línea. Disponible en: http://www.uncitral.org/uncitral/es/about_us.html. Consultada en Octubre 2008.

[84] Comercio Electrónico en Colombia. En línea. Disponible en: http://www.colombiestad.gov.co/index.php?option=com_docman&task=doc_details&gid=17&Itemid=97. 2007

[85] Verisign. Productos y servicios. Disponible en: http://www.verisign.com/latinamerica/esp/products-services/index.html. 2008

[86] GlobalSign. GMO Internet Group. Disponible en: http://www.globalsign.com/. 2008
[87] Third Party Certificate Authorities. Open Directory Project. Disponible en: http://www.dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities// . 2008
[88] Dirección de Impuestos y Aduanas Nacionales - DIAN. "Artículo 617 - Requisitos de la factura de venta". Estatuto Tributario. Junio 1996.
[89] Dirección de Impuestos y Aduanas Nacionales - DIAN. "Resolución No. 14465". Normatividad Técnica – DIAN. Disponible en: http://www.dian.gov.co/dian/13Normatividad.nsf/fa3eae82f6154e4a05256f88006679fd/69c2d8dfbea85aa5052573a20083879d?OpenDocument
[90] Asobancaria. Reporte de Bancarización a marzo de 2008. Vicepresidencia Económica. Dirección de Estudios y Regulación Financiera. CIFIN. Agosto de 2008.
[91] Banca de Oportunidades. Pagina Web. Disponible en: http://www.bancadelasoportunidades.gov.co/index.htm. Consultada en octubre de 2008.
[92] BID/FOMIN. Servicios Financieros a través de Tecnologías Móviles. Propuesta de consultoría al Programa de Apoyo a la Innovación (PAI) del Fondo General de Cooperación de España (FGCE) Regional. RG-T1501. 2008.
[93] Ministerio de Comunicaciones. Informe Trimestral de Telefonía Móvil TMC y PCS. trimestre julio a septiembre de 2008. Disponible en: http://www.mincomunicaciones.gov.co/mincom/src/index.jsp?page=./mods/contenido/view_page&id_contents=217&l=1
[94] Informe Sectorial de Telecomunicaciones. Comisión de Regulación de Telecomunicaciones. Bogotá D.C., Mayo 2008 - No. 10. Disponible en: http:// www.crt.gov.co.
[95] CINTEL Centro de Investigación de las Telecomunicaciones. Colombia. Noticintel Edición 673. Indicadores de TI. Antigüedad de los equipos que tienen los usuarios, Marzo de 2006. Disponible en: http://www.cintel.org.co/noticintel/noticia.php3?nt=4796&edicion=673.
[96] María del Rosario Guerra. Ministra de Comunicaciones de Colombia. Estrategias de Cierre de la Brecha Digital en Colombia: Plan de Gobierno en TICs 2006-2010. Miami, FL, mayo 31 de 2007.
[97] Galperin, H. Mariscal. Oportunidades Móviles: Pobreza y Telefonía Móvil en América Latina y el Caribe. DIRSI Dialogo Regional sobre Sociedad de la Información. Noviembre 2007

ANEXO A. PILOTO DE PRUEBA SEUS. CASOS DE USO DETALLADOS

1. Caso de Uso PAGAR

Pagar	
ACTOR:	Comprador
PROPOSITO:	Efectuar el pago de artículos mediante una interfaz de proximidad.
RESUMEN:	Inicia cuando el comprador pasa el móvil por el lector del POS, en ese momento se transmiten las credenciales de seguridad, almacenadas en la etiqueta al lector y luego del POS al AC, que obtiene la información de cuenta bancaria del usuario comunicándose con el AU, para conectarse con el Banco y enviarle la información necesaria para realizar la transacción. Finalmente se notifica al usuario y al POS si la transacción fue exitosa o únicamente a éste último si ocurrió algún error.
PRECONDICIONES:	• El móvil debe contar con interfaz RFID, el POS debe contar con conectividad a red. • Se deben generar o comprar los certificados necesarios en el AC y AU. • Se debe fijar las rutas de acceso a los certificados en los dos módulos mencionados. • Se debe fijar la información de acceso al Servidor de Directorio del AU, como dirección ip y puerto. • El usuario ha realizado un proceso previo de los artículos que va a adquirir.
ESCENARIO	Comprador 11. La etiqueta asociada al móvil se pasa por el lector y se realiza autenticación mutua entre ambos E1. 12. Se transmiten las credenciales almacenadas en la etiqueta. 13. Las credenciales se transmiten desde el POS al AC, E2. 14. Se fijan las rutas de acceso los certificados necesarios E3. 15. Petición de autenticación por parte del AC al AU, para el usuario que desea pagar. E4 16. Extraer información de cuentas bancarias alojadas en la cuenta de servicio en el AU. 17. Conexión con el Banco para solicitar que se efectúe la transacción. E5 18. Notificar resultado al POS. 19. Generación y envío de SMS al móvil del comprador. 20. Generación y envío de la factura digital a la cuenta de correo del comprador.
POSCONDICIONES:	Compra realizada

FLUJOS ALTERNATIVOS:	Ninguno
NOTAS:	Ninguna
EXCEPCIONES:	E1: No se puede realizar Autenticación Mutua. - No hay transferencia de credenciales. E2: El Cliente de Servicio no puede autenticarse. - No se puede establecer comunicación con el AC. E3: No se puede realizar comunicación sobre SSL. - No hay transferencia de credenciales. E4: La cuenta fue eliminada o suspendida. - El usuario es rechazado. E5: La red del Banco no está disponible. - Es imposible realizar la transacción.

Diagrama de Clases

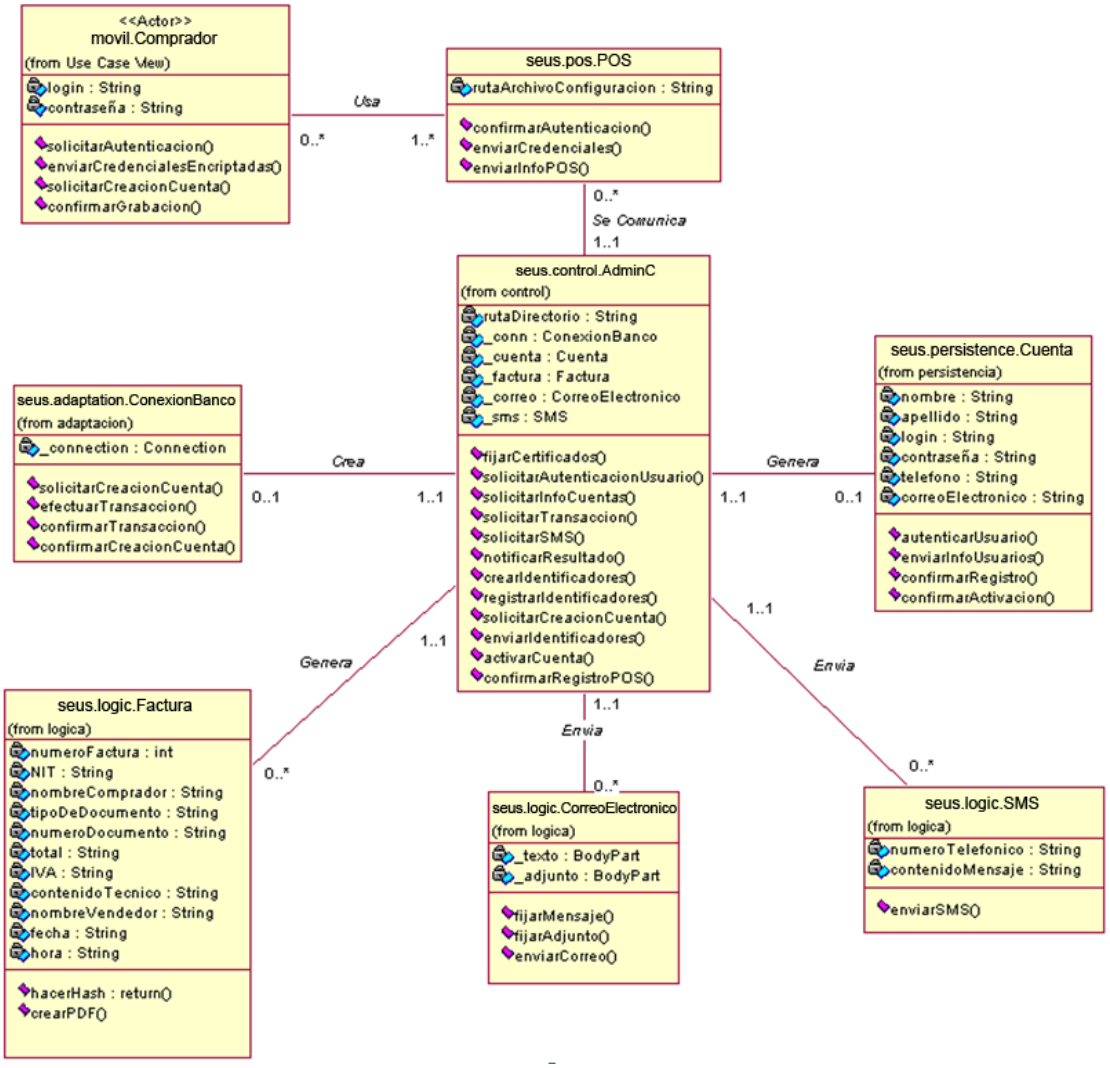
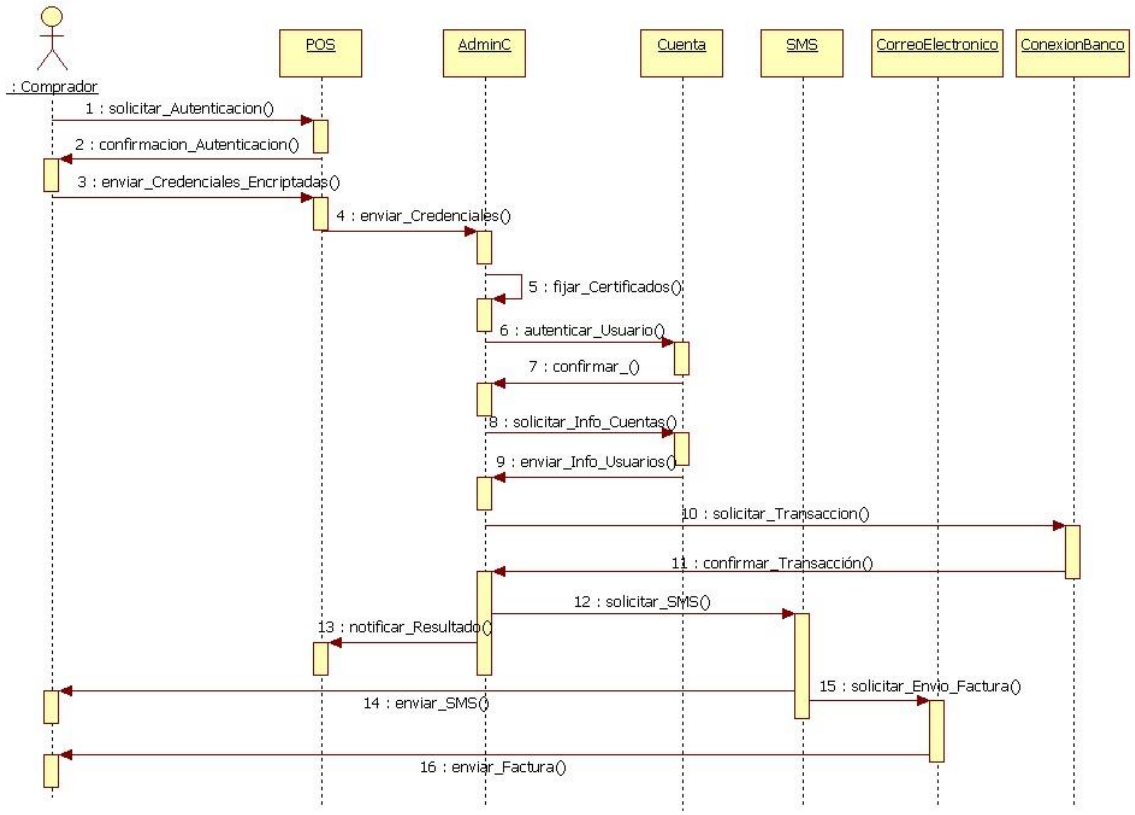


Diagrama de Secuencia



2. Caso de Uso Solicitar Creación Cuenta

Solicitar Creación Cuenta	
ACTOR:	Comprador
PROPÓSITO:	Crear una cuenta de servicio para que el comprador pueda usar el servicio de pago por proximidad.
RESUMEN:	La información personal necesaria del usuario es recolectada en el PCC y enviada al AC, el cual genera una credencial para el usuario y crea una nueva cuenta de servicio para comprador en el AU con la información recibida, para luego realizar una petición de creación de cuenta bancaria al Banco. Finalmente se envía al PCC la información que debe ser grabada en la etiqueta RFID.
PRECONDICIONES:	• Se deben generar o comprar los certificados necesarios en el AC y AU. • Se debe fijar las rutas de acceso a los certificados en los dos módulos mencionados. • Se debe fijar la información de acceso al Servidor de Directorio del AU, como dirección ip y puerto. • Acuerdo con el banco para permitir la interconexión y el intercambio de solicitudes.
ESCENARIO	Comprador 1. El usuario solicita la creación de cuenta en un PCC, para acceder al servicio de pago. 2. Se envía la información personal del usuario desde el PCC al AC E1. 3. El AC genera de clave de cuenta del usuario que será almacenada en el AC y en la etiqueta. 4. El AC registra toda la información del usuario en una cuenta del AU, E2. 5. Se solicita al banco la creación de una cuenta bancaria, en la cual el banco define un tope máximo diario. 6. Se envían los identificadores (nombre de usuario y clave generada) al PCC. 7. Se graba el nombre del usuario y la clave generada en la etiqueta RFID. 8. El PCC confirma la grabación al AC. 9. El AC activa la cuenta en el AU. 10. Se confirma la activación de la cuenta.
POSCONDICIONES:	Cuenta creada
FLUJOS ALTERNATIVOS:	Ninguno
NOTAS:	Ninguna
EXCEPCIONES:	E1 El Cliente de Servicio no puede autenticarse. - No se puede establecer comunicación con el AC.

	E2: No se puede realizar comunicación sobre SSL - No hay transferencia de credenciales.

Diagrama de Clases

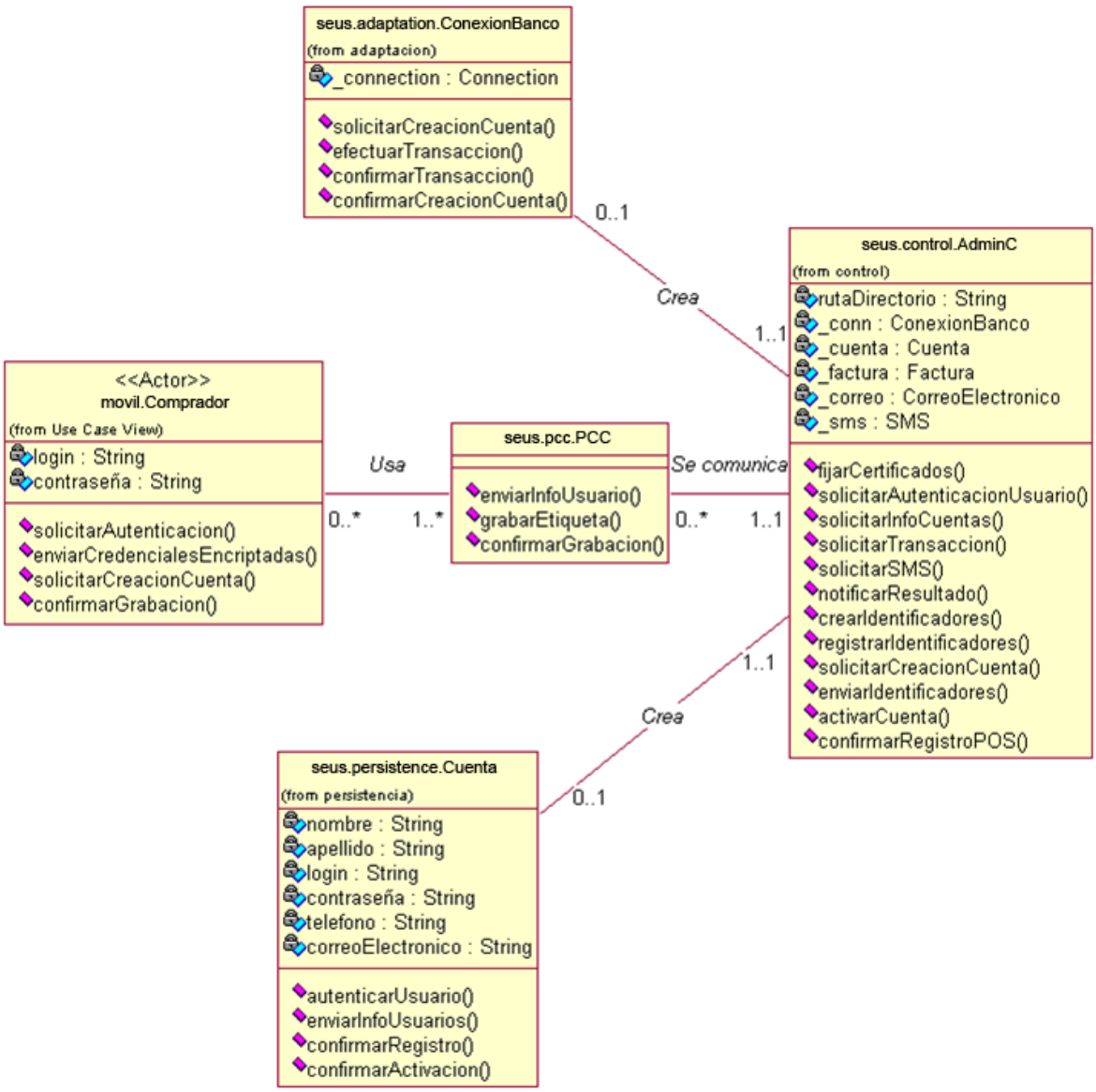
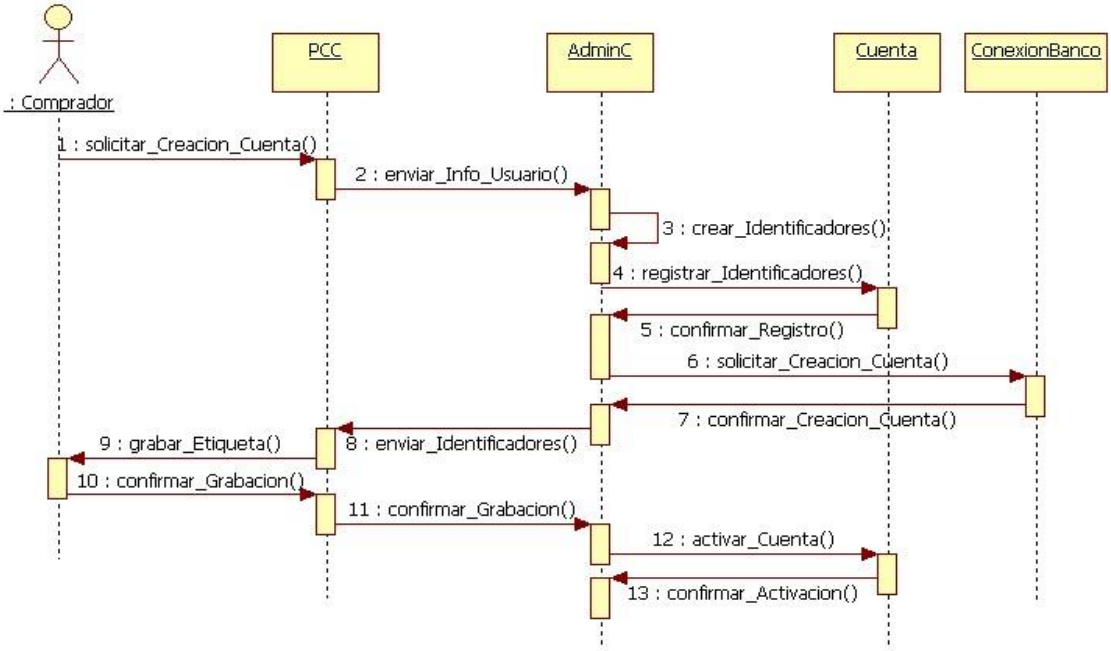


Diagrama de Secuencia



3. Caso de Uso Registrar POS

Registrar POS	
ACTOR:	Vendedor
PROPOSITO:	Registrar el Punto de Pago asignándole una cuenta de servicio con el fin de habilitar la recepción de pagos por proximidad en un establecimiento.
RESUMEN:	La información necesaria del establecimiento comercial es recolectada en el POS y enviada al AC, el cual genera una credencial para ese POS en particular y crea una nueva cuenta de servicio para vendedor con la información recibida. Una vez registrada correctamente esta información, se notifica al POS que el registro fue satisfactorio.
PRECONDICIONES:	• Se deben generar o comprar los certificados necesarios en el AC y AU. • Se debe fijar las rutas de acceso a los certificados en los dos módulos mencionados. • Se deben fijar la información de acceso al Servidor de Directorio del AU, como dirección ip y puerto.
ESCENARIO	Comprador 1. El vendedor por medio de un POS envía su información personal E1. 2. El AC genera la contraseña de cuenta de servicio del POS, que hace parte de las credenciales del mismo. 3. El AC registra toda la información del POS en una cuenta del AU, E2. 4. El AC notifica al POS que el registro se realizó correctamente.
POSCONDICIONES:	Cuenta de Servicio del Vendedor Creada
FLUJOS ALT.:	Ninguno
NOTAS:	Ninguna
EXCEPCIONES:	E1 El Cliente de Servicio no puede autenticarse. - No se puede establecer comunicación con el AC. E2: No se puede realizar comunicación sobre SSL - No hay transferencia de credenciales.

Diagrama de Clases

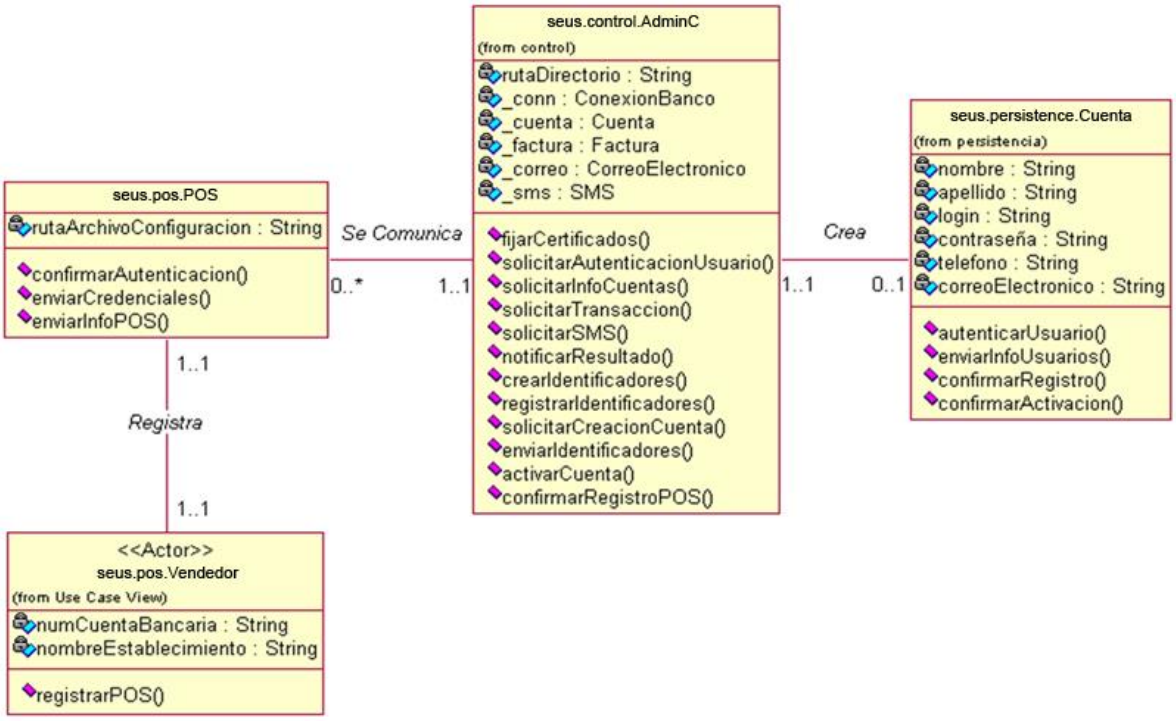
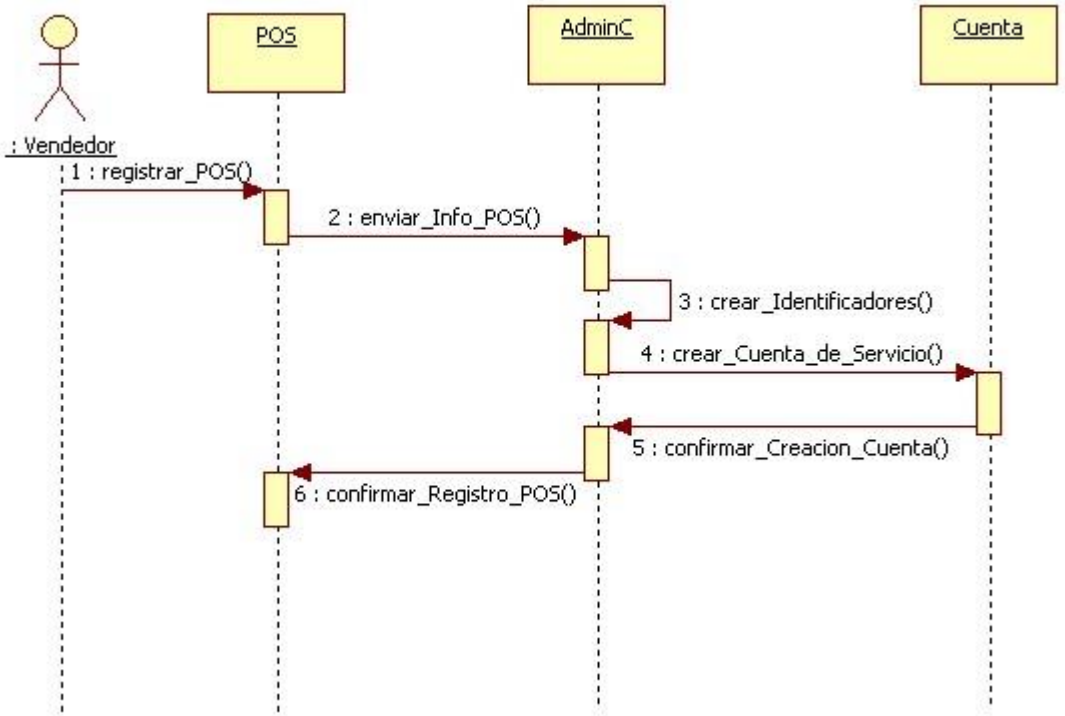


Diagrama de Secuencia



ANEXO B. DESCRIPCION DETALLADA DE LAS PRUEBAS

1. Pruebas de seguridad

- **Pruebas de Scanning**

Para llevar a cabo la búsqueda de puertos en los equipos, se empleó la herramienta nmap de la distribución Backtrack. En la Figura 1 se muestran los resultados obtenidos al escanear el AC, donde se puede apreciar que está corriendo un Servicio Web al ver los puertos 8080 y 8082 abiertos:

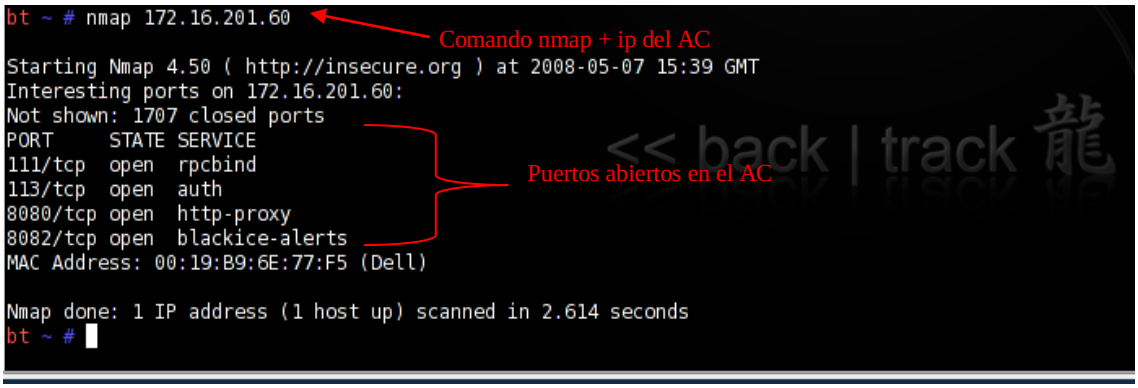


Figura 1. Mapeo del AC

En la Figura 2 se muestran los resultados obtenidos al escanear el AU, donde se aprecia el puerto 636 abierto, el cual es utilizado por el servidor LDAP en modo seguro.

Figura 2. Mapeo del AU

Este análisis que permite hacer nmap a los servidores AC y AU es aparentemente pasivo e inofensivo, pero puede convertirse en el primer paso de un ataque que concluya con la des habilitación de cualquiera de los dos servidores. Por lo anterior es importante y fundamental instalar un firewall que impida este tipo de ataques y así bloquear cualquier tipo de amenaza desde el principio. De este modo tanto en el servidor AC como en el AU se configuró el firewall firestarter, que es idóneo para servidores que tengan Debian como Sistema Operativo. Al hacer la búsqueda de puertos en el AC con el firewall activado se obtienen los resultados mostrados en la Figura 3, en la cual se puede apreciar que no es posible visualizar los puertos abiertos:

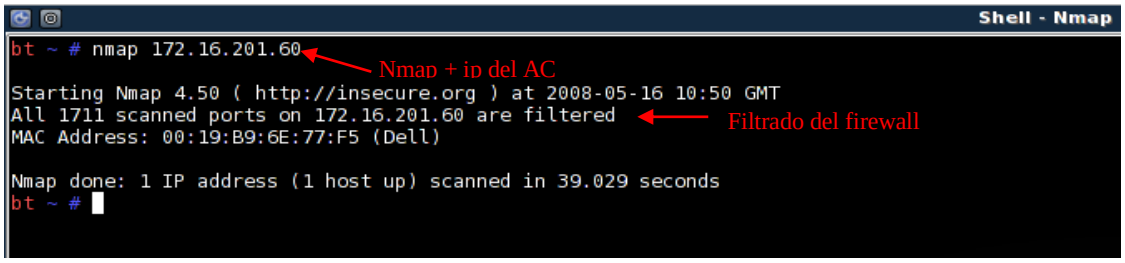


Figura 3. Mapeo del AC con el Firewall activado

Los resultados al mapear el AU y el POS con el firewall activado fueron similares y se muestran en la Figura 4 y 5 respectivamente.

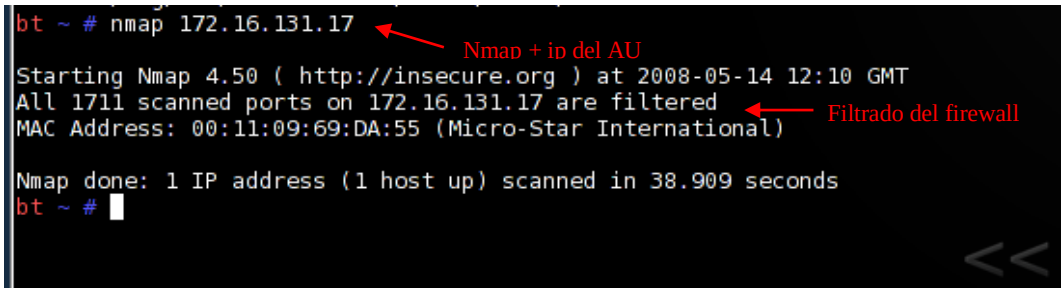


Figura 0. Mapeo del AU con el firewall activado

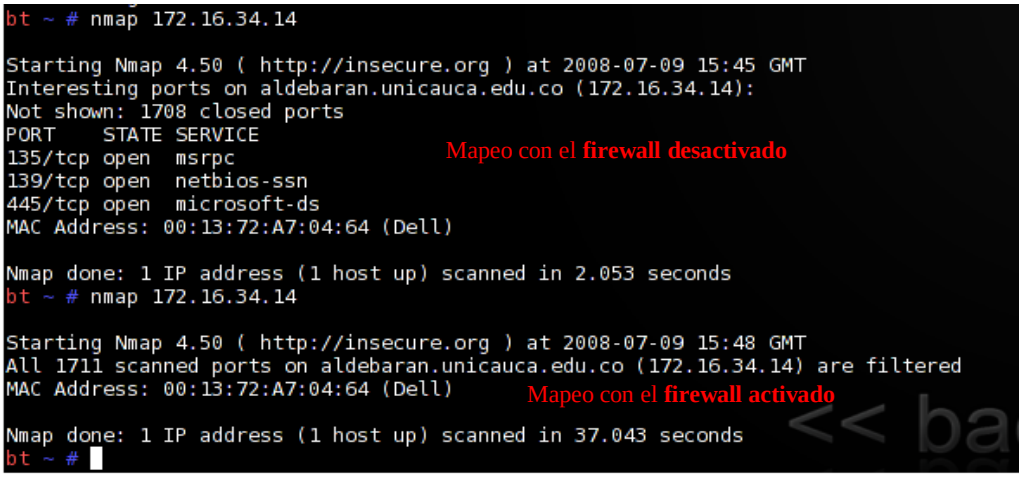


Figura 5. Mapeo del POS

Las Figuras 3, 4 y 5 muestran los resultados obtenidos en el equipo desde el cual se está intentando hacer la búsqueda, pero en los Servidores AC y AU el firewall Firestarter notifica sobre estos intentos de ataque, como se muestra en la Figura 6.

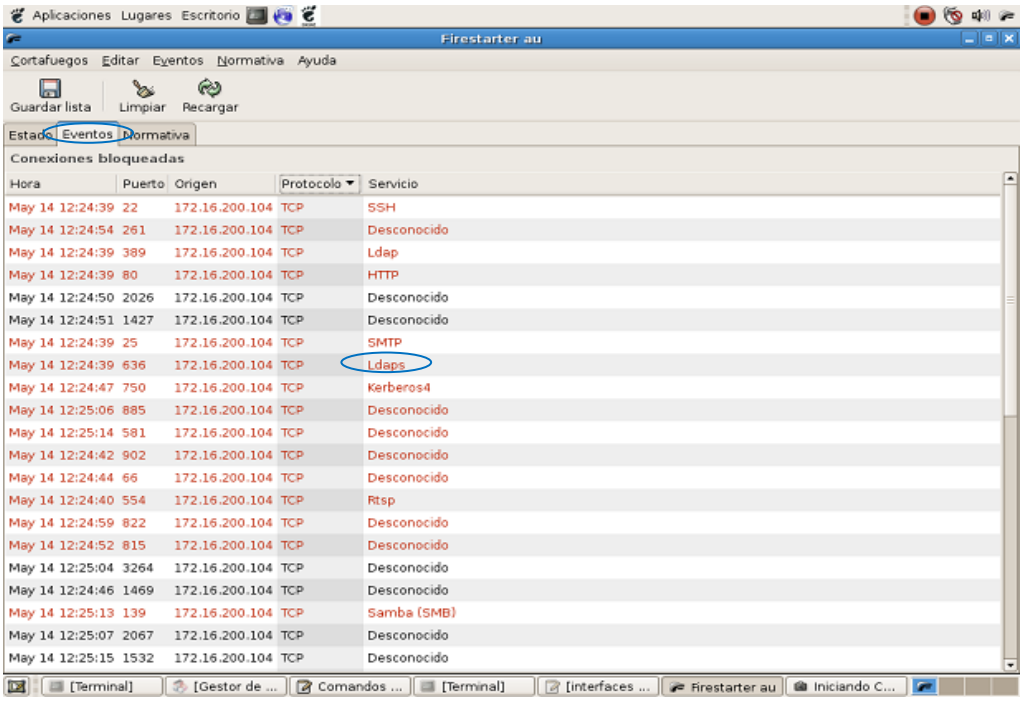


Figura 6. Eventos detectados por el Firewall en el AU

- **Pruebas de Sniffing**

Para el monitoreo y análisis de tráfico entre los equipos del sistema se empleó la herramienta wireshark, también incluida en la distribución backtrack. Primero se analizó el tráfico entre el AC y el AU para demostrar que los datos transferidos están cifrados. Un servidor LDAP puede trabajar en dos modos, uno inseguro donde la información se transporta en texto plano a través del puerto 389, y otro seguro donde se manejan certificados y la información va cifrada a través del puerto 636. Por obvias razones el servidor LDAP del AU de SeUS se configuró en modo seguro, pero para notar la diferencia entre ambos, se hicieron pruebas en los dos modos. En la Figura 7 se muestra la interfaz de wireshark, herramienta que empieza un análisis automático de toda la red una vez es lanzado, por lo cual se realiza un filtro especificando la dirección IP de interés.

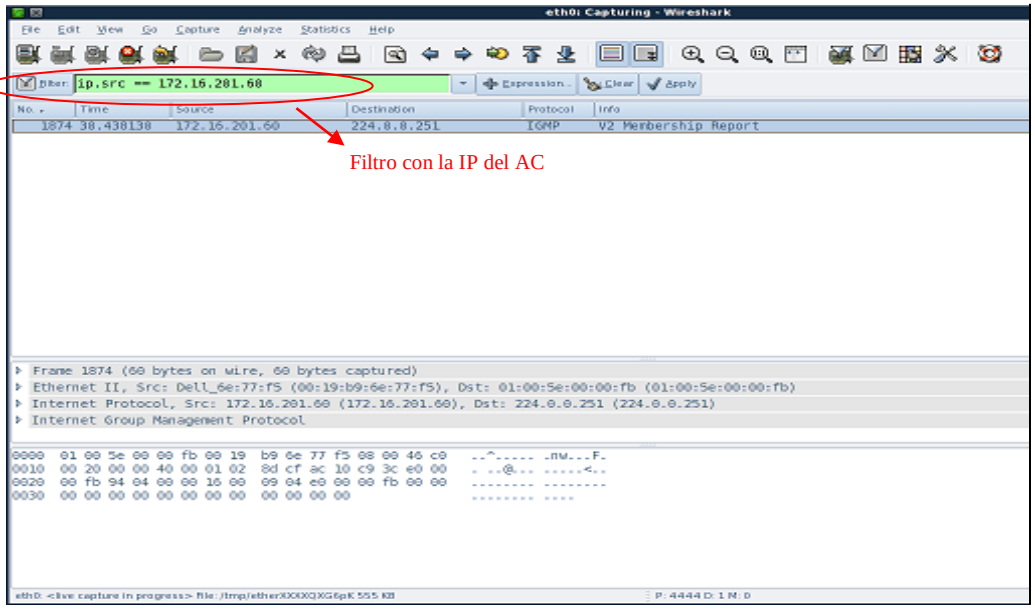
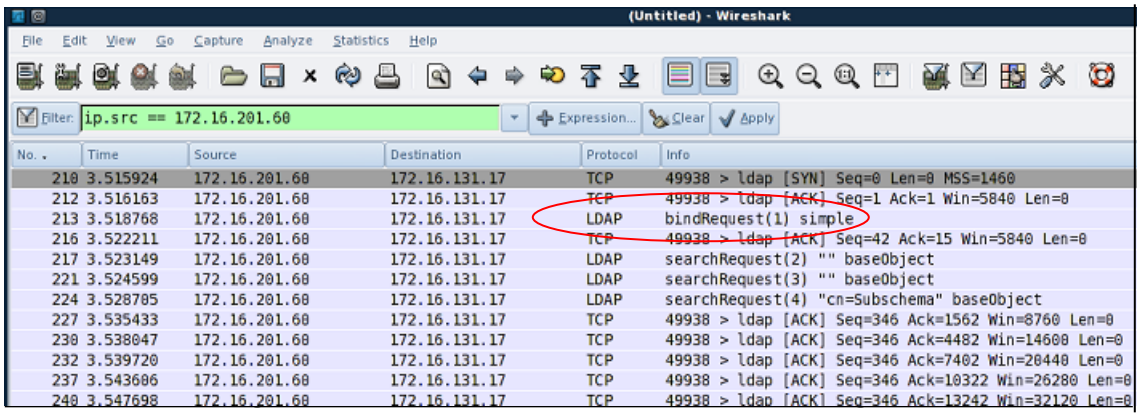


Figura 7. Interfaz de Wireshark

Al monitorear el tráfico con el LDAP en modo inseguro se puede ver con claridad cada una de las acciones realizadas sobre el AU, por ejemplo la conexión (Ver Figura 8) y la desconexión (Ver Figura 9).



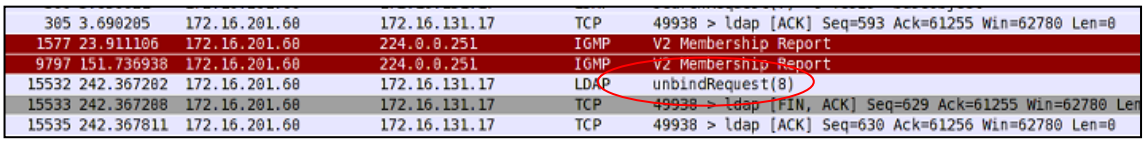


Figura 9. Solicitud de Desconexión en modo inseguro

En modo inseguro no solo se pueden apreciar las operaciones sobre el directorio LDAP, sino información más detallada como el directorio al cual se hace la conexión (Ver Figura 10). También se hizo una prueba modificando datos de las cuentas del directorio, en donde se visualizan los datos insertados y la información del usuario seleccionado (Ver Figura 11), que demuestran lo inseguro de este modo de operación.

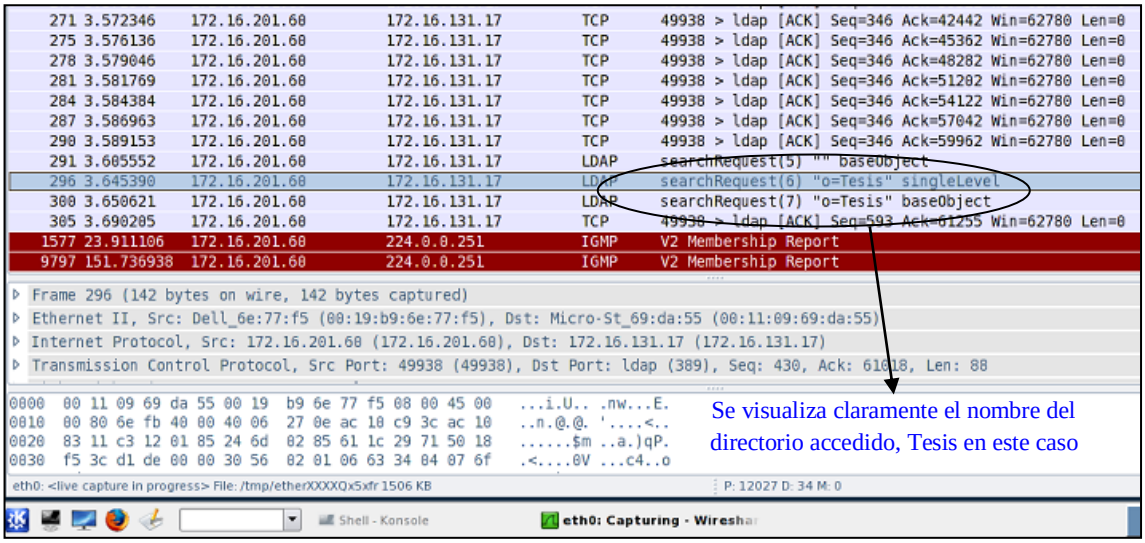


Figura 10. Información obtenida de LDAP en modo inseguro

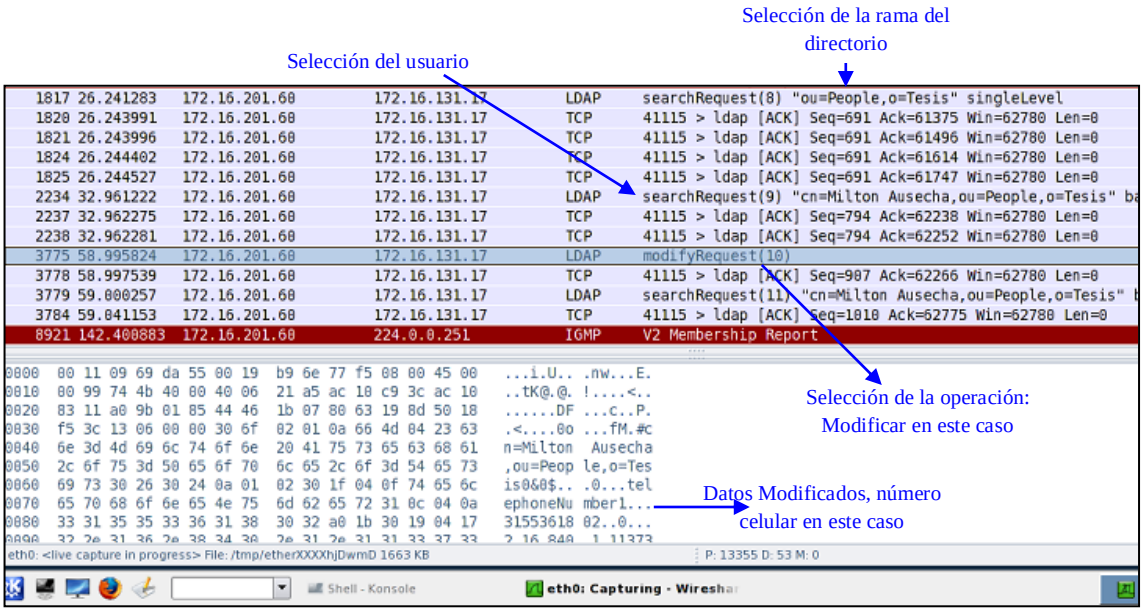


Figura 11. Modificación de datos en el AU en modo inseguro

Las pruebas anteriores en el modo inseguro se hicieron con el fin de ser comparadas con el modo seguro y entender mejor el funcionamiento de este último. El Servidor LDAP del AU de SeUS siempre va a correr en modo seguro por los requerimientos que implica un servicio de pago. Se hicieron las mismas pruebas en modo seguro y se obtuvo que es imposible visualizar las operaciones que se llevan a cabo, debido al manejo de certificados y del protocolo TLS en el Servidor. La Figura 12 es una conexión a LDAP, donde la herramienta notifica una operación en el directorio LDAP en modo seguro, que utiliza TLS y cifrado de datos, pero en ningún momento muestra el nombre del directorio accedido y el tipo de operación. La Figura 13 muestra una modificación hecha en una cuenta del directorio y se puede apreciar que la notificación para cualquier operación: conexión, desconexión, modificación, inserción, etc, es la misma, utilizando

un mensaje Application Data. Tampoco se ve información de usuario en texto plano como en el modo inseguro, y los únicos datos que se pueden visualizar además de identificar una conexión LDAP en modo seguro, son las direcciones IP de los dos equipos implicados en la comunicación, AC y AU en este caso.

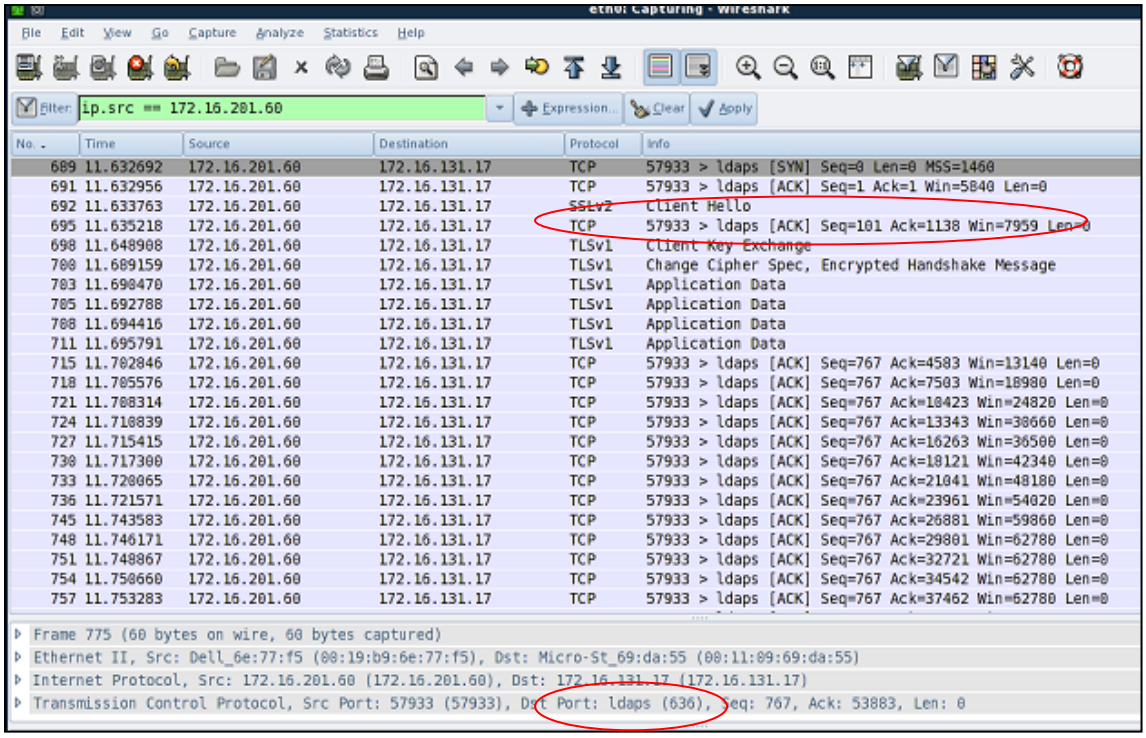


Figura 12. Conexión a LDAP en modo seguro

Después de husmear las comunicaciones entre el AC y el AU, se hizo lo mismo entre el AC y el POS/PCC. El servidor Web del AC, al igual que el directorio LDAP, puede funcionar en un modo seguro y en otro inseguro. La prueba realizada consistió en crear una nueva cuenta de vendedor, obteniendo que en modo inseguro absolutamente todos los datos se transfieren en texto plano, como se puede apreciar en las Figuras 14 y 15.

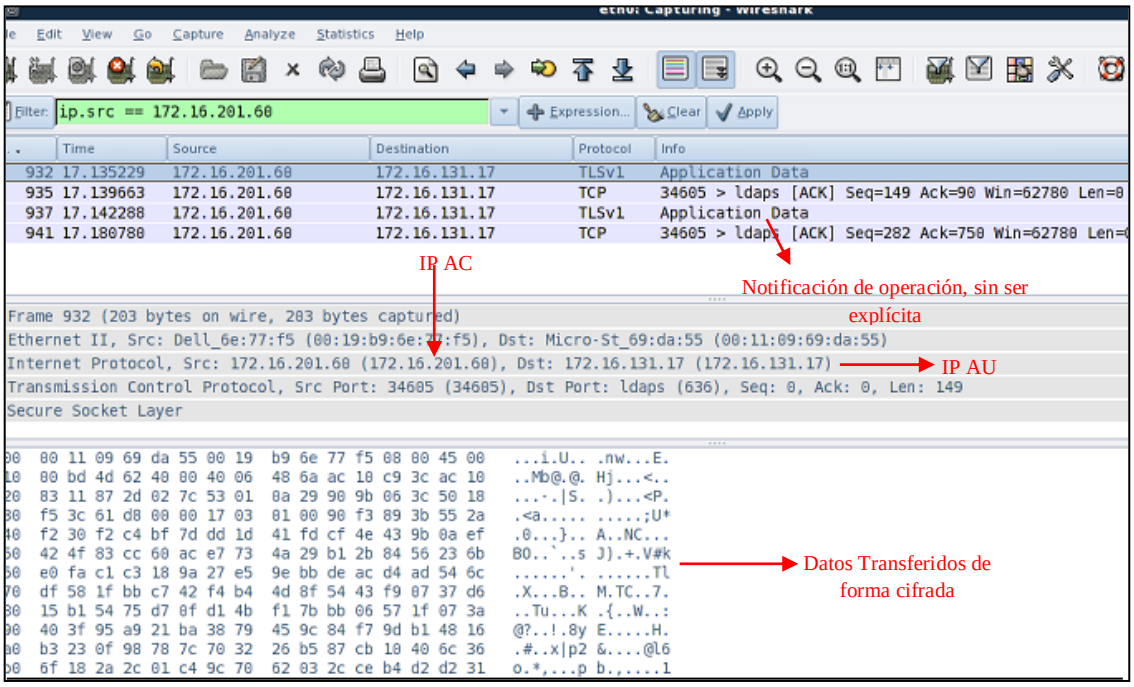


Figura 13. Operaciones sobre LDAP en modo seguro

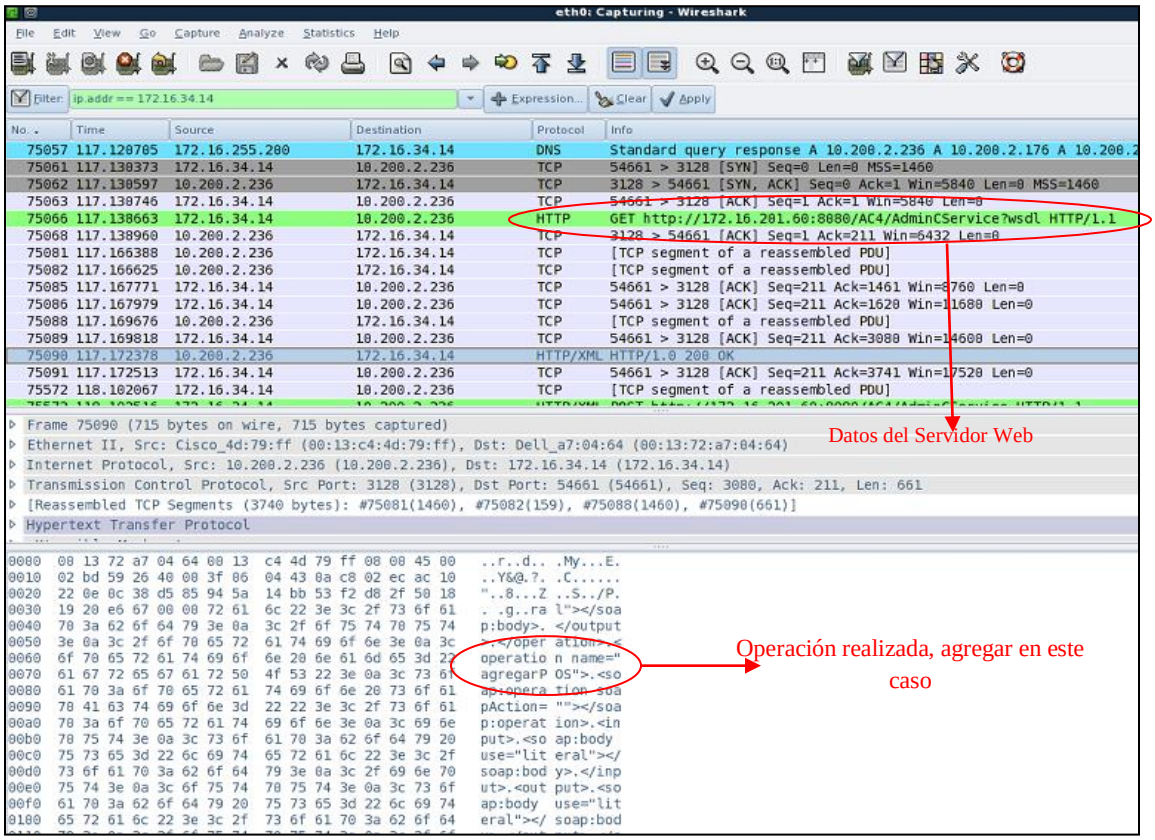


Figura 14. Comunicación POS/PCC-AC en modo inseguro

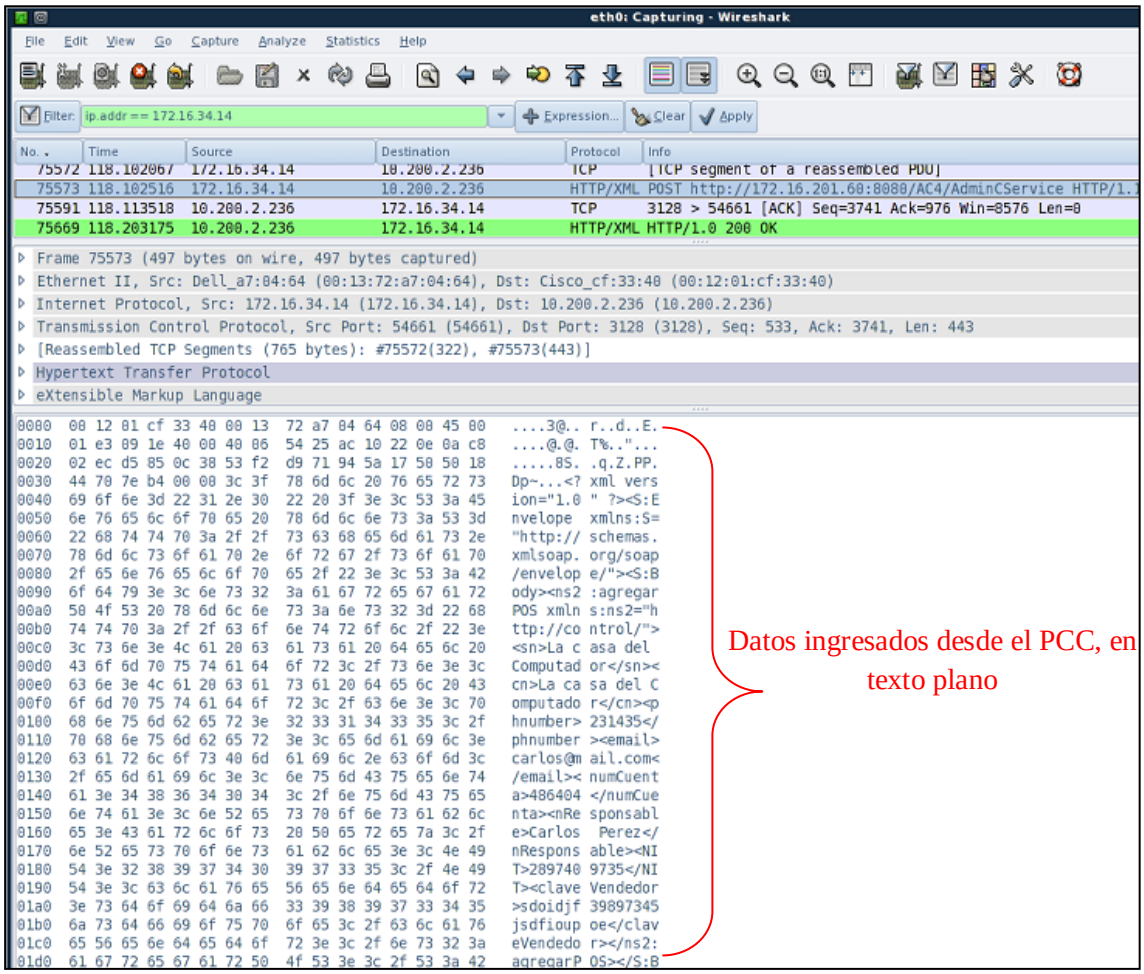


Figura 15. Transferencia de Datos PCC/POS-AC en modo inseguro

Luego se reinició el Servidor Web del AC en modo seguro y al escanear la comunicación no se visualizan los datos enviados desde el PCC, ya que estos están cifrados, como se muestra en las Figura 16. Ni siquiera la operación realizada se puede identificar, a parte de los datos generales del servidor como la IP, ninguna otra información es suministrada.

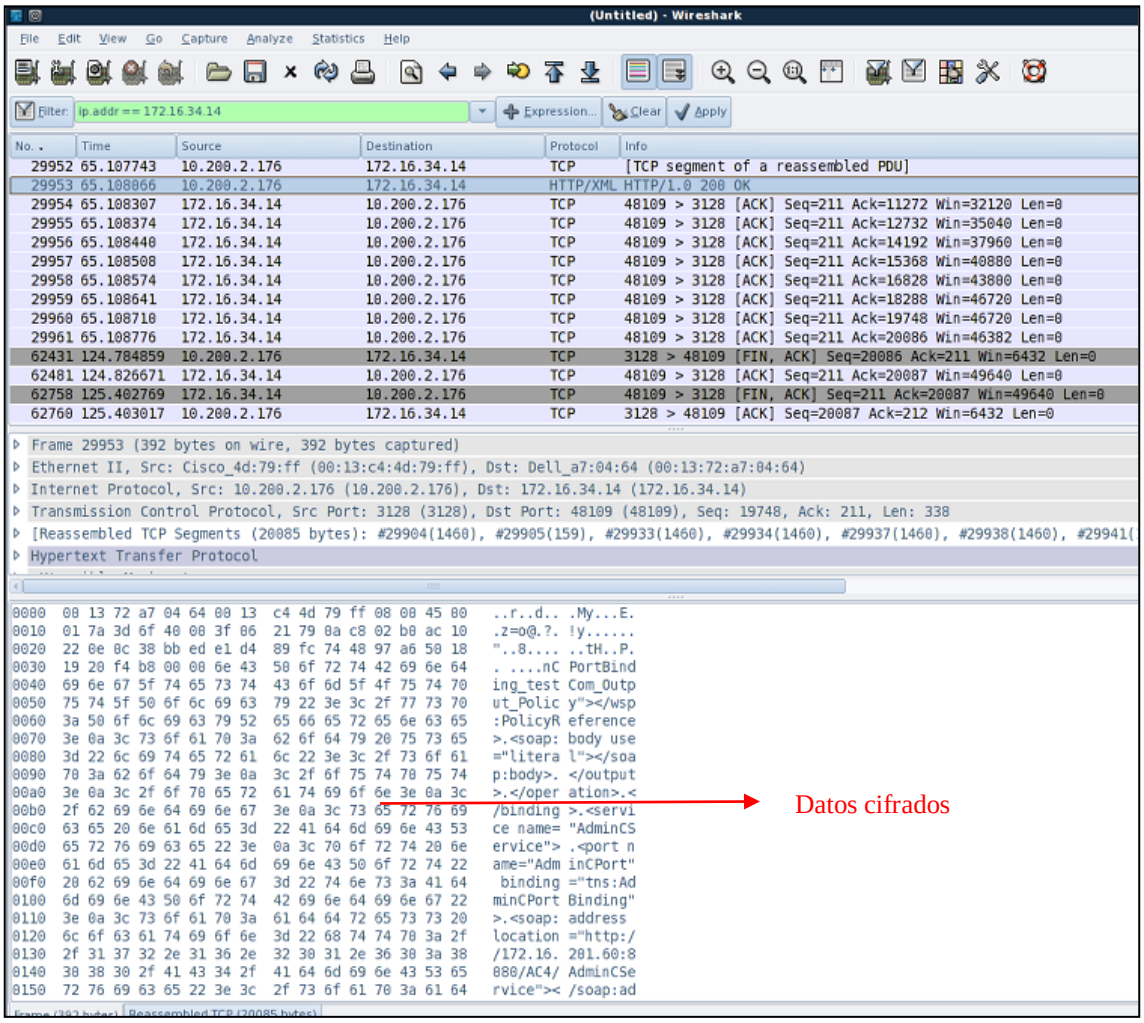


Figura 16. Comunicación segura entre POS/PCC y AC

- **Pruebas de Spoofing**

Es una técnica de ataque consistente en suplantar a una entidad de una red con el fin de recibir información confidencial. Las dos entidades escogidas para esta prueba fueron el AC y el AU, donde se suplantó a este último por medio de la herramienta Ettercap.

Ettercap es una herramienta con interfaz gráfica, contenida en Backtrack, diseñada especialmente para pruebas de spoofing, pero que permite otro tipo de ataques como Sniffing y Denial of Service. Una vez se abre la interfaz de ettercap el primer paso es seleccionar la opción sniff/unified sniffing, donde se escoge la interfaz de red utilizada para el ataque. Después de esto se activa un escaneo de la red mediante la opción Hosts/Scan for host y después de unos minutos en la ruta Host/Host list aparecen las direcciones IP y MAC de todos los equipos encontrados en la red, como se muestra en la Figura 17.

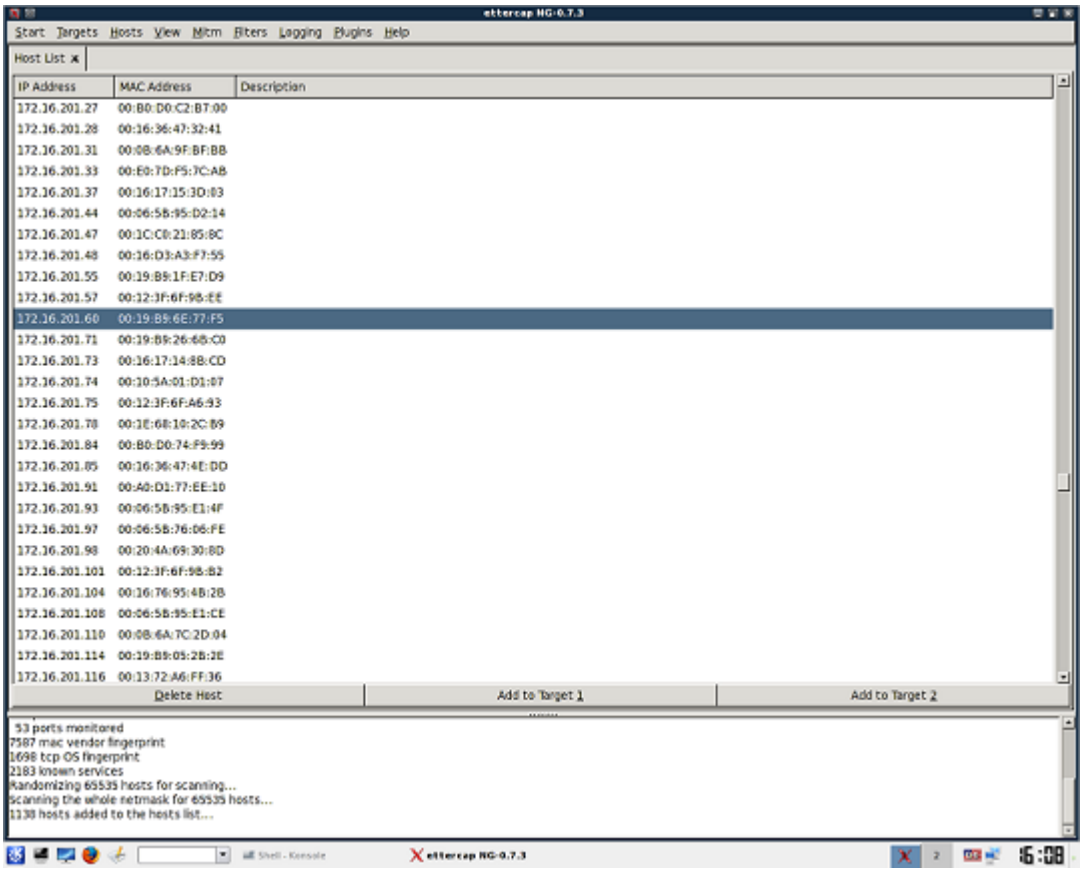


Figura 17. Listado de host disponibles en ettercap

Del listado de hosts mostrados por ettercap se deben seleccionar los dos equipos entre los cuales se desea interceptar la comunicación, en primer lugar se escoge el equipo fuente de los datos y después el que se quiere suplantar. En la prueba realizada se hizo pasar el equipo intruso por el AU, y así recibir información enviada desde el AC (Ver Figura 18). Después se escoge el tipo de spoofing, en este caso se trata de uno basado en direcciones IP y MAC, para lo cual se selecciona la ruta MITM/ARP Poising/remote.

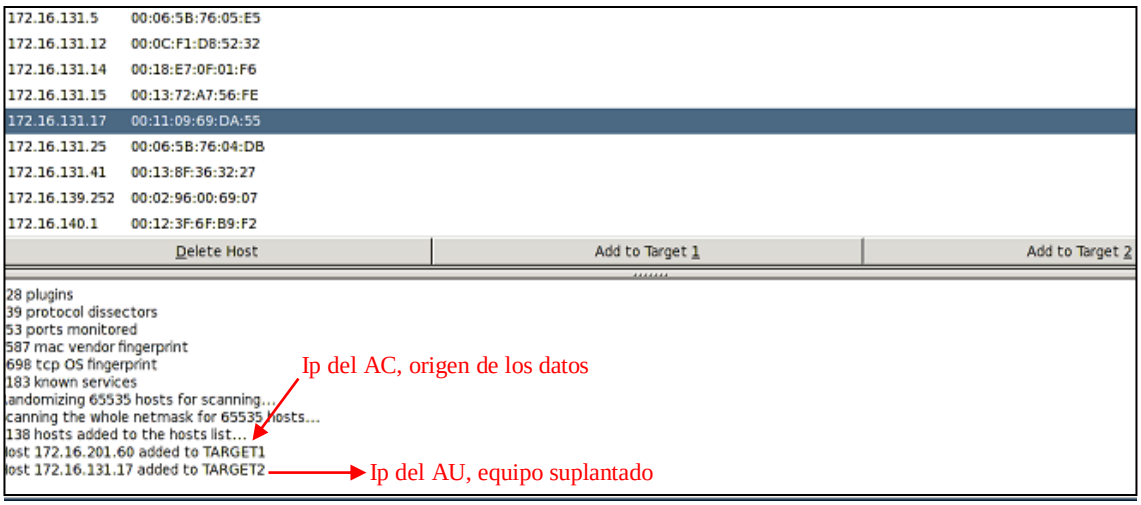


Figura 18. Selección de los dos equipos para el spoofing

La suplantación empieza con un sniffing de la red, proceso que se activa en la opción start/start sniffing del menú. Después de habilitar esta opción aparece en la parte de abajo una notificación que confirma el sniffing y además al seleccionar la ruta view/connections se puede ver la información intercambiada entre los dos equipos escogidos (Ver Figuras 19 y 20).

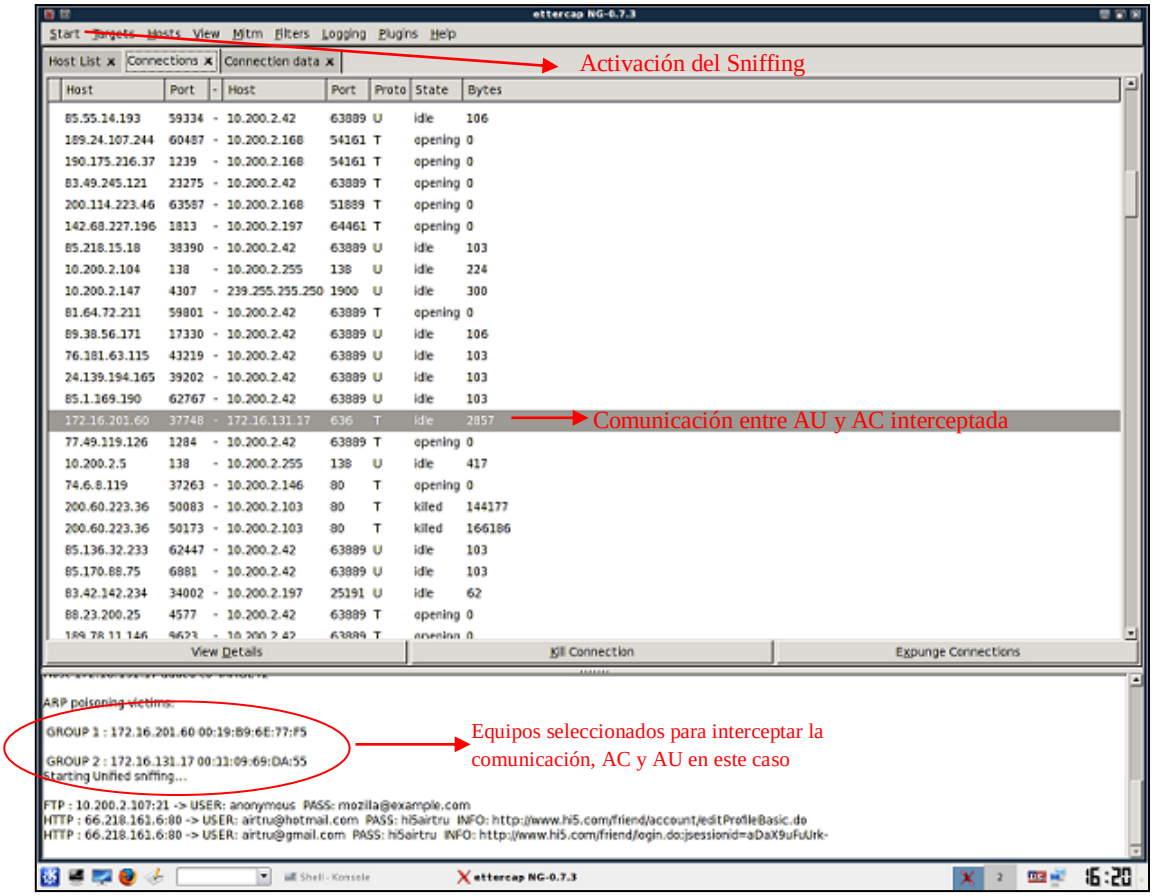


Figura 19. Activación del Sniffing

En la Figura 20 se observa que la información interceptada va cifrada, como se había comprobado con wireshark. La diferencia es que ettercap puede husmear comunicaciones que se encuentren en dominios diferentes de red, además no solo intercepta datos, sino que los recibe al estar suplantando a otro equipo, incluyendo llaves de seguridad, por lo cual con las herramientas y algoritmos suficientes se podría descifrar la información. Este no es un proceso sencillo y por el contrario requiere la intervención de un experto, sin embargo representa un riesgo para el sistema, por lo que se debe implementar una solución que permita una comunicación segura basada en una autenticación previa de las entidades involucradas en ella. En SeUS se implementó una VPN, con la herramienta software openvpn, con el AC como servidor, y el POS y el AU como clientes, que impide la conexión de intrusos a equipos del servicio al solicitar una autenticación inicial. Todo el proceso de configuración de la VPN se expone en el Anexo C.

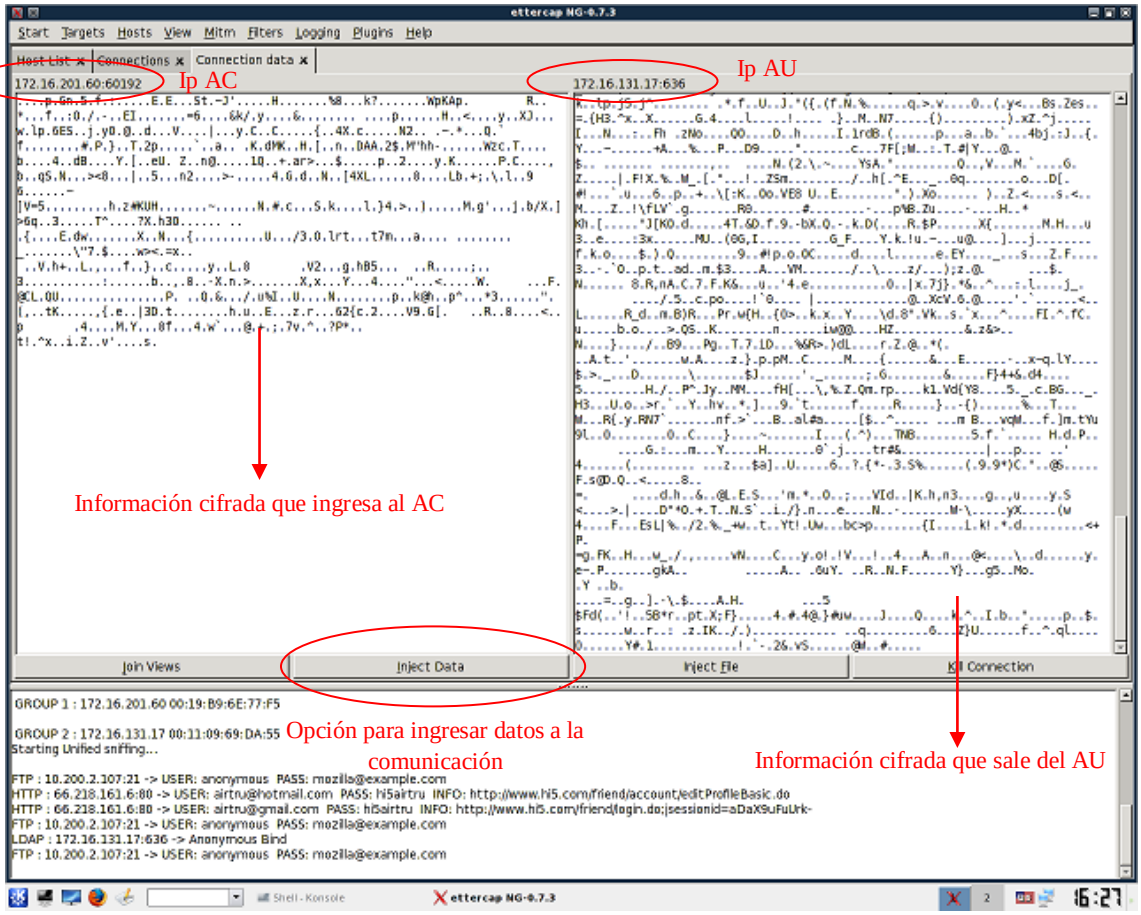


Figura 20. Conexión interceptada en ettercap

La Figura 21 muestra como un intento de suplantación entre el AC y el AU es inútil cuando la VPN está activada. Las IP virtuales del AC y el AU son 172.16.50.1 y 72.16.50.2 respectivamente, ettercap a pesar de que es capaz de identificar estas dos interfaces en su escaneo de equipos, no puede interceptar la comunicación entre ellos, caso contrario a lo que pasaba con las interfaces originales como se observó en la Figura 19.

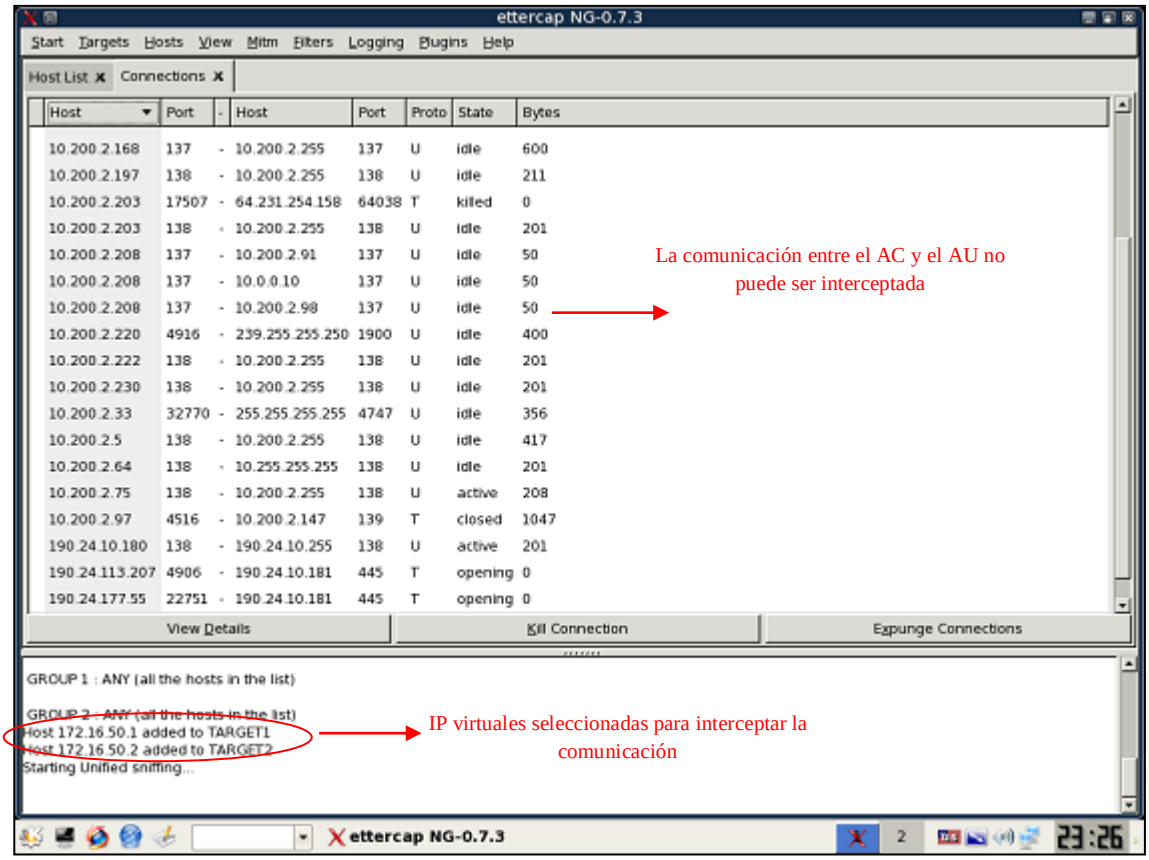


Figura 21. Intento de suplantación entre el AC y el AU con la VPN activada

- **Pruebas de denegación de servicio**

Ettercap fue diseñada para ataques tipo spoofing, pero también facilita otras operaciones sobre una comunicación interceptada, como su eliminación, que desencadenaría la no prestación del servicio, razón por la cual se empleó como herramienta para un ataque de denegación de servicio. En muchas ocasiones el atacante no tiene el conocimiento y las herramientas para descifrar la información, entonces opta simplemente por interrumpir la comunicación y así alterar la prestación del servicio, prueba que fue llevada a cabo en SeUS como se observa en la Figura 22. Para comprobar la interrupción de la comunicación se intentó acceder al directorio LDAP del AU desde el AC, mediante la herramienta gráfica JXplorer_LDAP, y el resultado fue el no acceso al servidor como se aprecia en la Figura 23. Ettercap también permite la inserción de datos en la comunicación, facilitando la generación de una sobrecarga en el enlace, que es otra forma de ataque de Denegación del servicio (Ver Figura 24). Aunque el desenlace es diferente al del ataque spoofing, el origen es el mismo, la ausencia de un mecanismo robusto de autenticación que impida la suplantación de una entidad, por lo cual la solución también es una VPN.

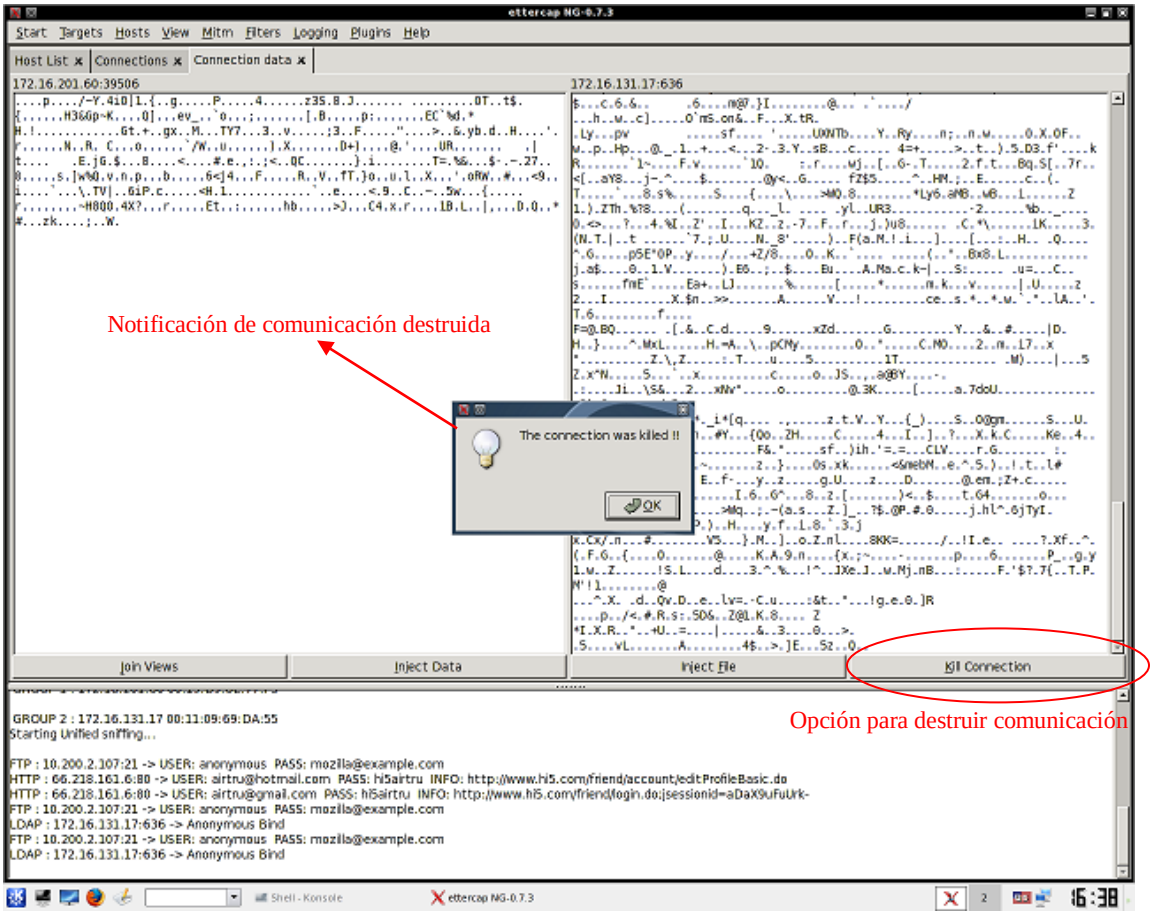


Figura 22. Destrucción de una Comunicación con ettercap

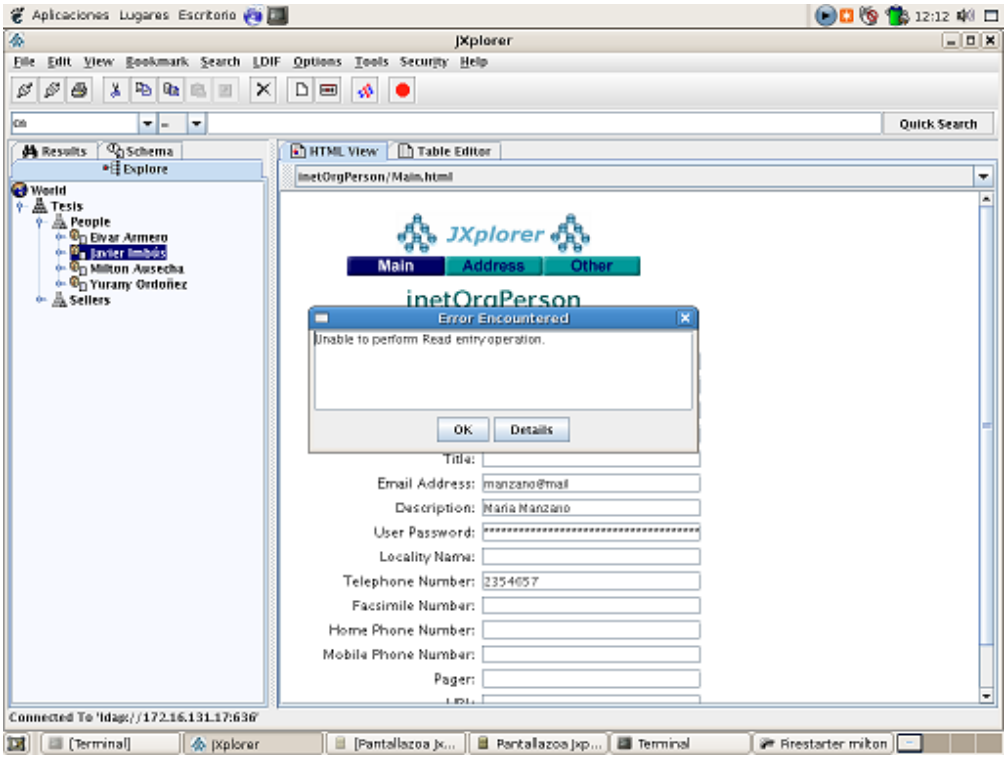


Figura 23. Acceso denegado empleando JXplorer_LDAP en el AC

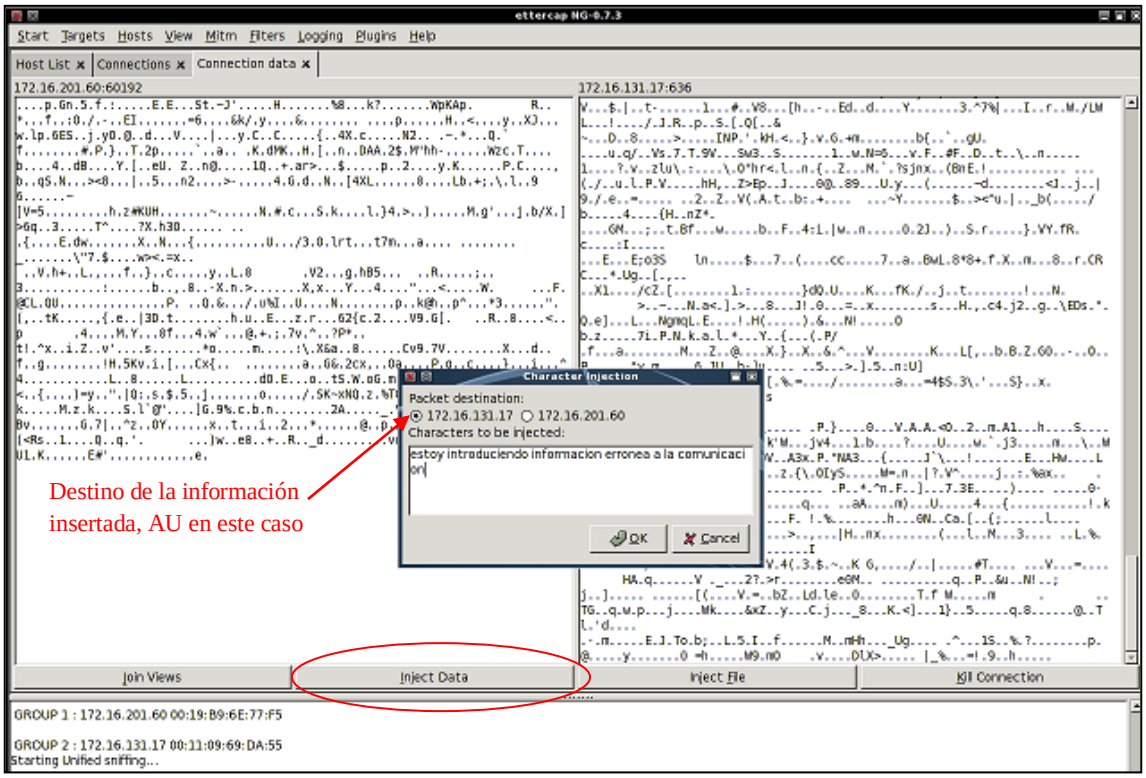


Figura 24. Denegación de servicio por inserción de datos

- **Pruebas de Exploits**

Un exploit es un programa que aprovecha una vulnerabilidad de un equipo para alterar el funcionamiento de un servicio o aplicación. En las pruebas de seguridad de SeUS se empleó la herramienta Metasploit, incluida en Backtrack. Los sistemas operativos y software en general progresan día a día con mayor rapidez, y los exploits no son ajenos a esta evolución, por lo cual antes de cualquier ataque de este tipo, es necesario actualizar los repositorios de exploits como se muestra en las Figuras 25 y 26.

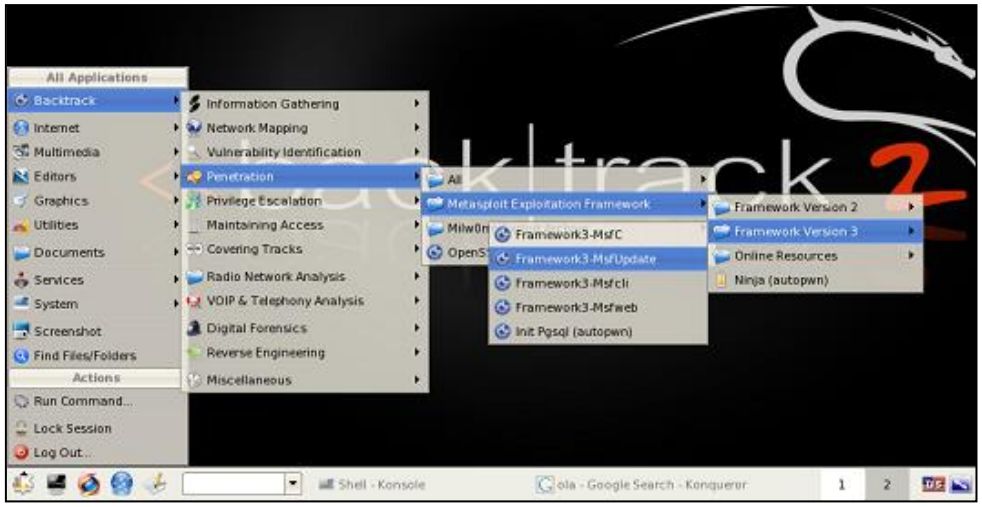


Figura 25. Activación de la Actualización de Exploits.

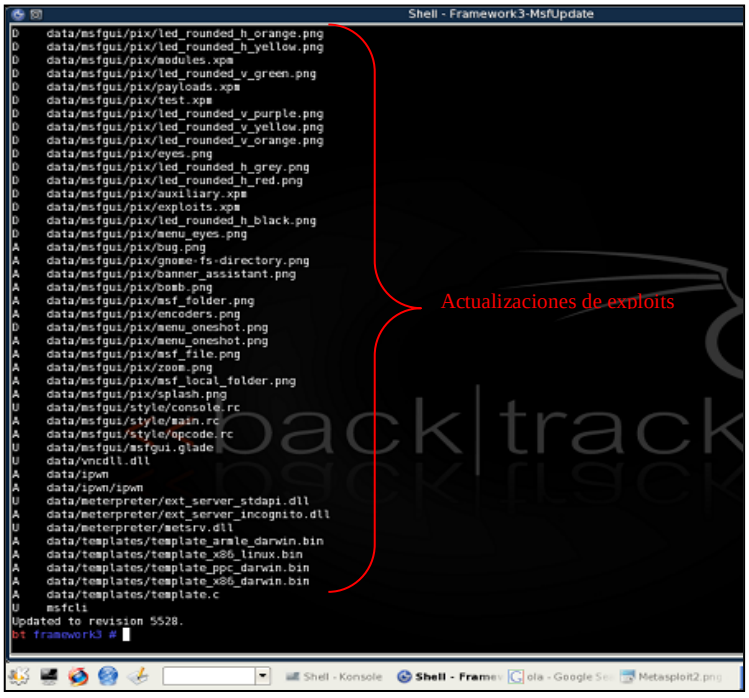


Figura 26. Finalización de la actualización de exploits

Una vez actualizado el repositorio de exploits se accede a la ruta mostrada en la Figura 27, después de lo cual empezará el ataque (Ver Figura 28). Lo primero que hace Metasploit es una búsqueda de los equipos que pertenecen a la misma red del equipo atacante, para lo cual ejecuta nmap automáticamente (Ver Figura 29). Por lo anterior se debe configurar la interfaz del equipo desde el cual se ataca, en la misma red del Servidor atacado.

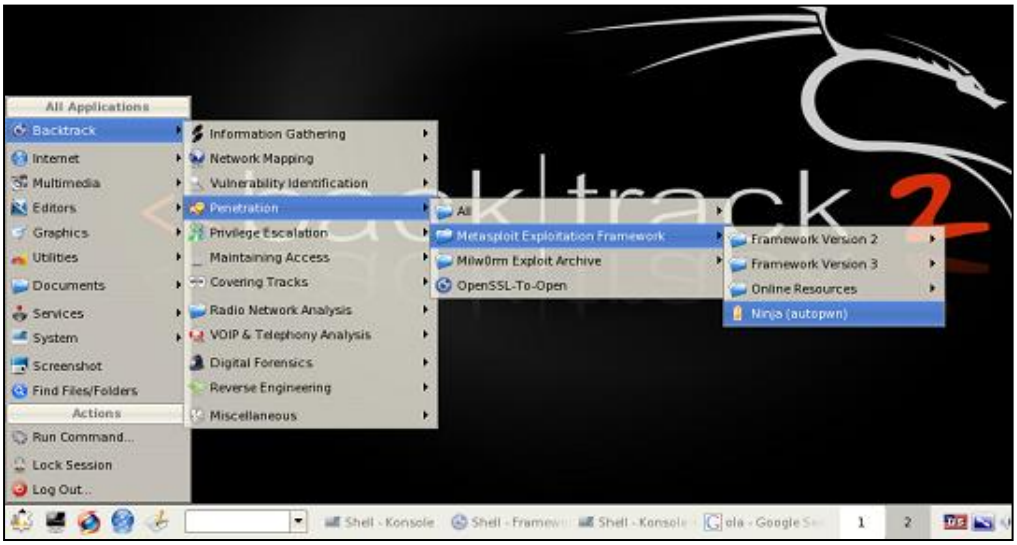


Figura 27. Activación del ataque

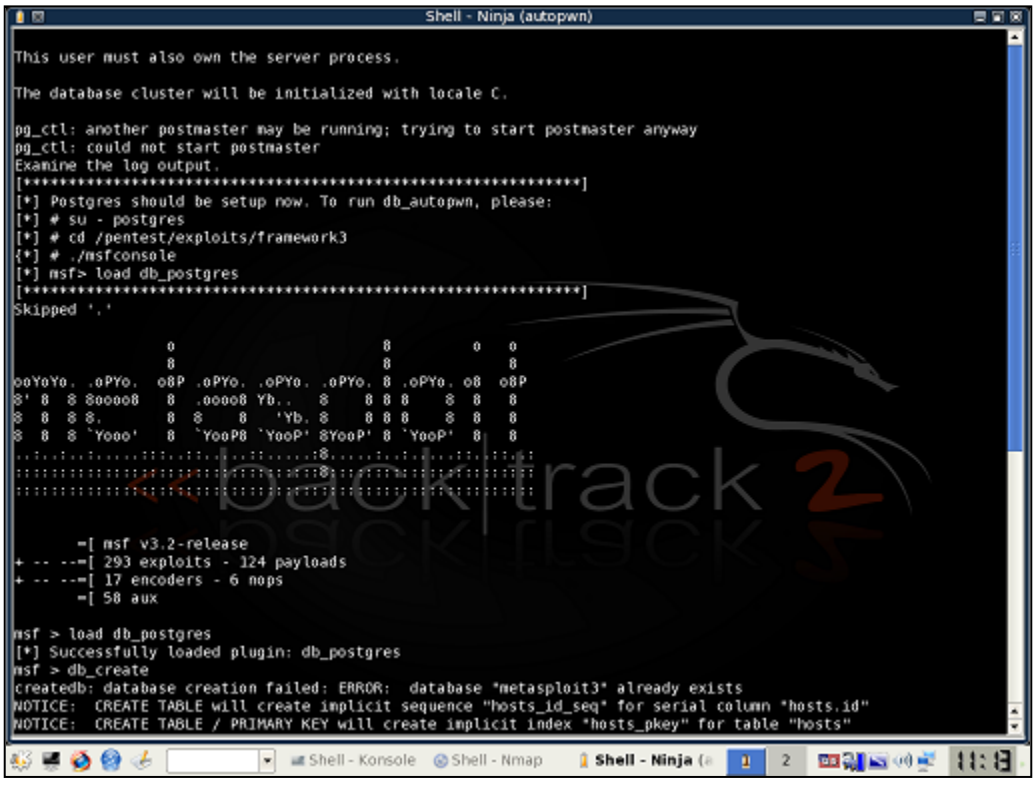


Figura 28. Inicio del ataque

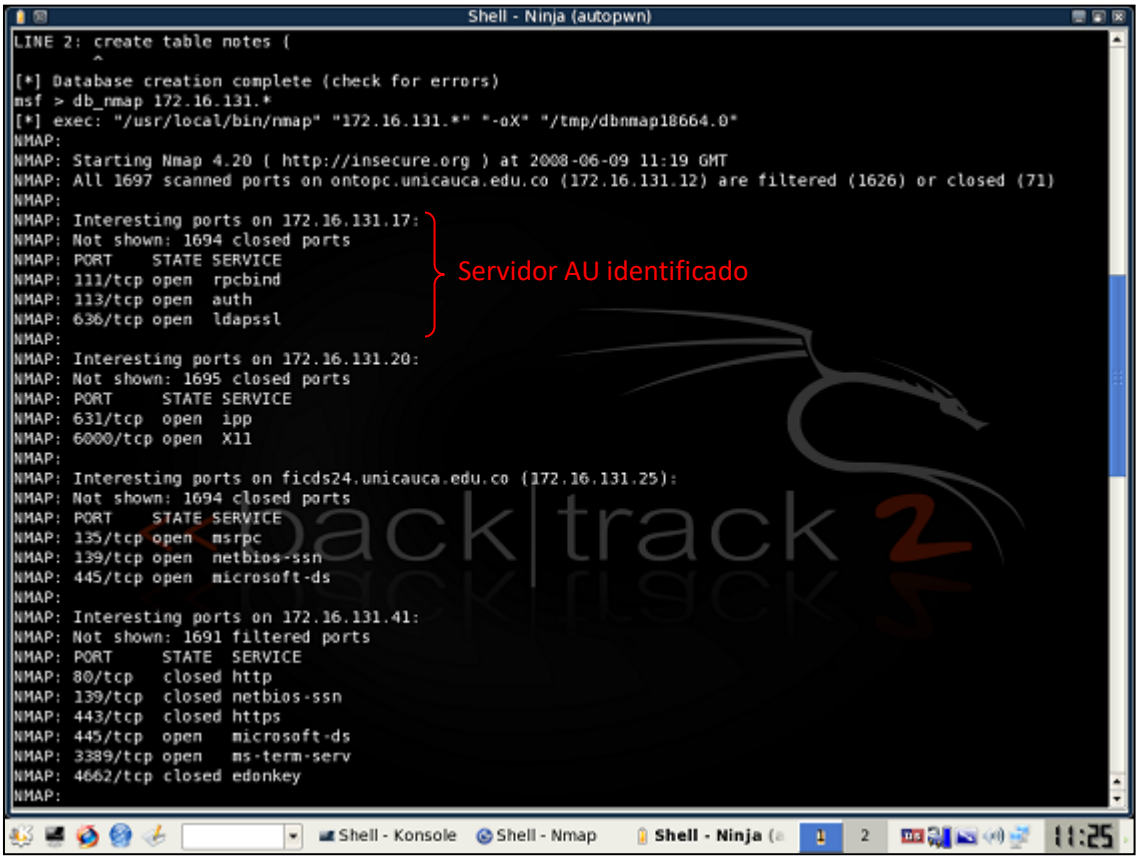


Figura 29. Búsqueda inicial de equipos

Después de la búsqueda de equipos comienza la ejecución de cada uno de los exploits en todos los hosts detectados. Al realizar el ataque a los servidores AC y AU de SeUS con Metasploit actualizado a 8 de Junio de 2008 se obtuvieron buenos resultados de seguridad, es decir ninguno de los exploits tuvo éxito. Las Figuras 30, 31 y 32 muestran varios de los intentos de ataque fallidos tanto al AC como al AU. Así actualmente no se encuentren exploits que afecten a SeUS, en cualquier momento puede aparecer una amenaza para este sistema, por lo cual es importante evitar este tipo de ataques, y si se tiene en cuenta que ellos empiezan con la ejecución de nmap, la solución la provee el firewall ya instalado en los servidores. Los resultados de las pruebas de exploits mostrados hasta ahora se hicieron con el firewall desactivado, pero si se activa, la herramienta Metasploit ni siquiera puede detectar al equipo en la búsqueda inicial, como se muestra en la Figura 4.36, y si no se detecta el servidor, no se puede lanzar ningún exploit contra él.

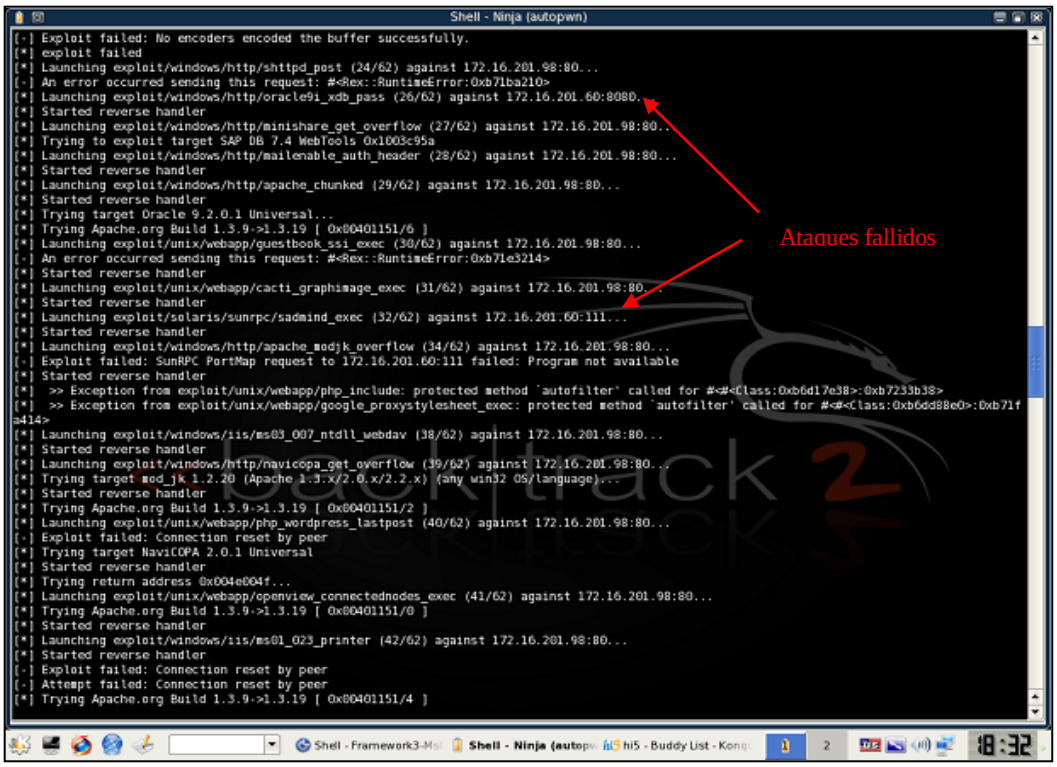


Figura 30. Ataques fallidos al AC

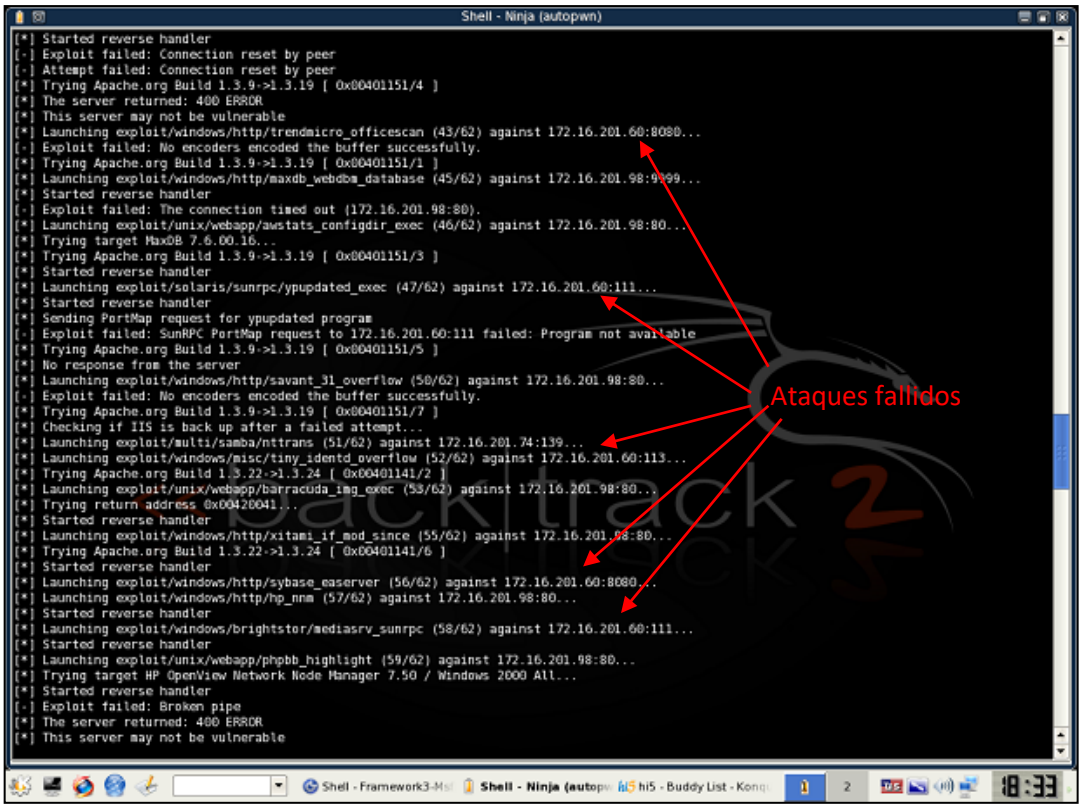


Figura 31. Ataques fallidos al AC

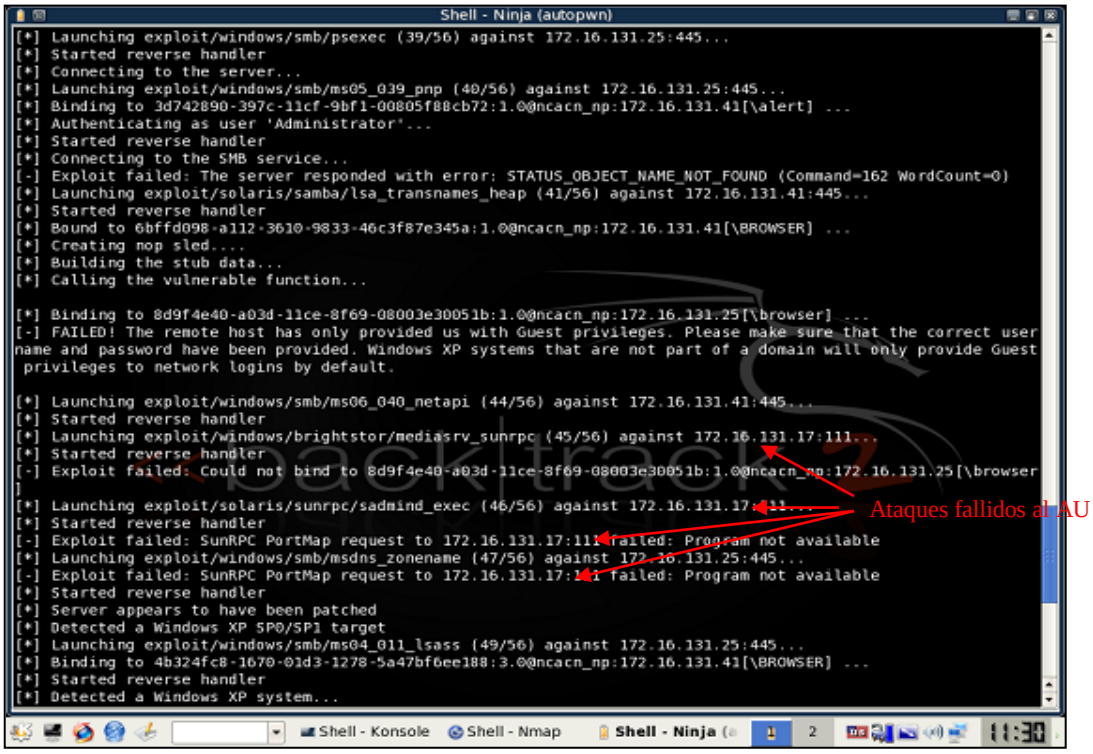


Figura 32. Ataques fallidos al AU

La Figura 33 muestra el funcionamiento de Metasploit con el firewall activado. Si se tiene en cuenta que los hosts identificados se muestran en forma ascendente, y que la dirección del AU es 172.16.131.17, se puede observar que no se detecto el servidor.

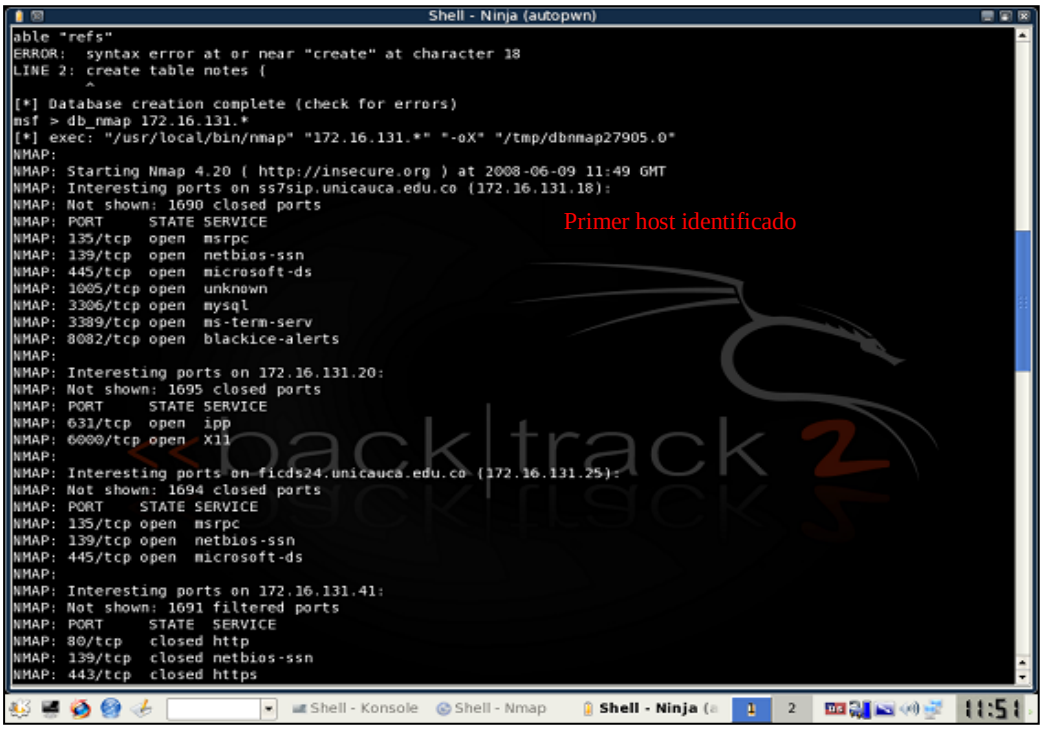


Figura 33 Metasploit con el firewall activado

El firewall genera un reporte de los intentos de mapeo realizados desde el equipo intruso con Metasploit. La Figura 34 muestra las alertas generadas en el servidor atacado.

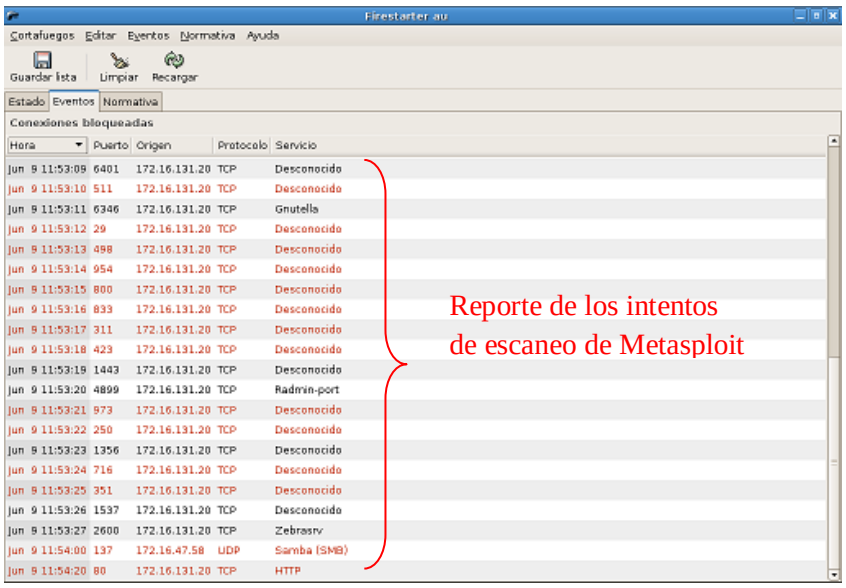


Figura 34. Reporte de Alertas generados por el firewall ante los exploits

2. Eficiencia en SeUS

El tiempo de procesamiento de la información y la memoria consumida son dos aspectos importantes en cualquier desarrollo software, por lo cual son analizados en SeUS. Las aplicaciones del AC y el POS fueron desarrolladas en Netbeans, razón por la cual se utilizó la herramienta Netbeans Profiler para analizar las propiedades mencionadas.

- **Eficiencia del AC**

Tiempos de procesamiento

En la Figura 35 se muestran los resultados al realizar un análisis del servicio del AC con Netbeans Profiler, en donde se aprecia que el tiempo máximo que tarda el servicio Web para empezar a atender solicitudes, una vez compilado, es 45.2 ms.

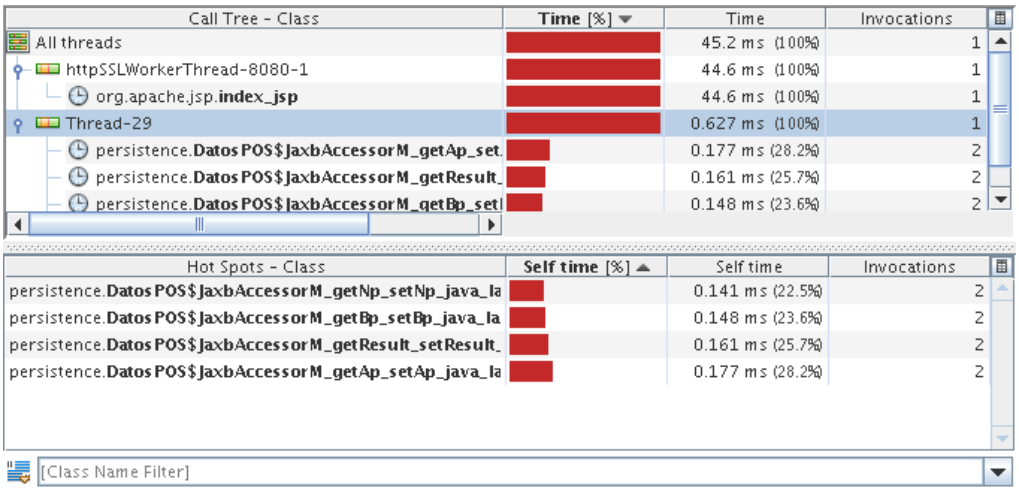


Figura 35. Tiempo de procesamiento del AC

Consumo de Memoria

Es importante que una aplicación Web sea ligera, para evitar fallas debidas a la indisponibilidad de recursos suficientes para su ejecución. En la Figura 36 se muestra que una vez lanzado el servicio, el consumo de memoria empieza a crecer alcanzado un pico de 50 Megas, pero en un tiempo aproximado de 40 segundos el consumo se estabiliza en 30 Megas, que es un valor bastante bajo respecto a la memoria disponible. En la Figura 36 la región morada representa la memoria consumida y la rosada la que se encuentra disponible, y como se puede apreciar la segunda siempre es superior a la primera.

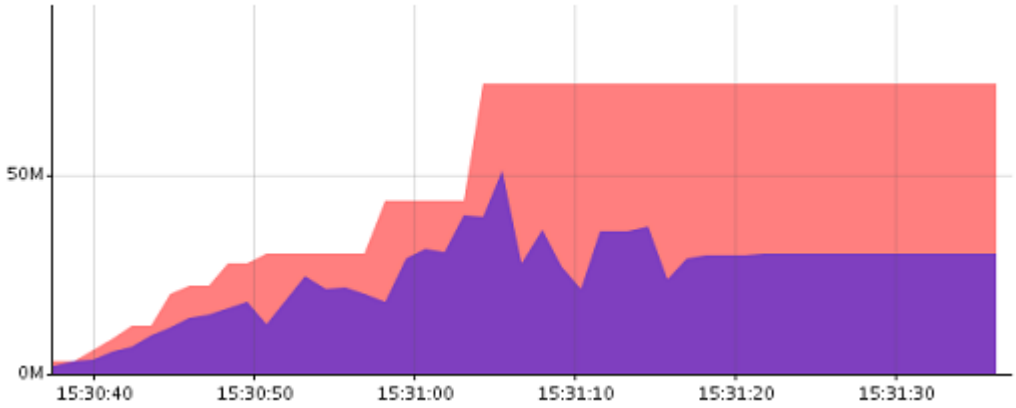


Figura 36. Consumo de memoria del servicio en el AC

El momento en que el consumo de memoria se estabiliza corresponde al período de tiempo durante el cual el servidor está esperando solicitudes de los clientes, que se ve alterado cuando el PCC o el POS requieran un servicio, como se aprecia en la Figura 37. Se crearon varias cuentas y se realizaron varios pagos de forma seguida, obteniendo un leve aumento en el consumo de memoria durante el período que se llevaron a cabo estos procesos, como se muestra en la Figura 38.

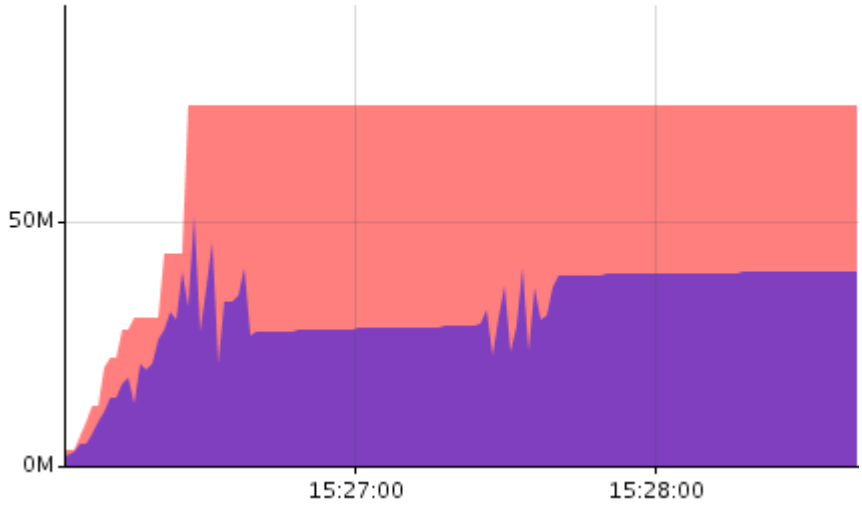


Figura 37. Consumo de memoria en una solicitud al AC

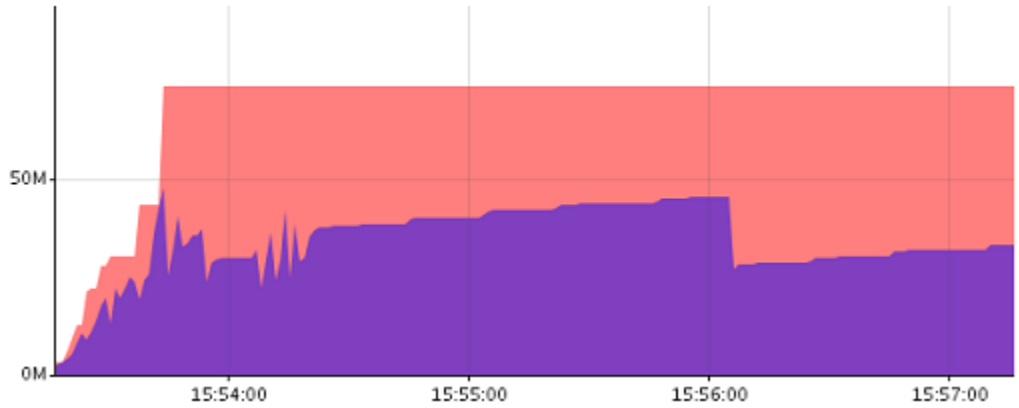


Figura 38. Consumo de memoria con solicitudes sucesivas al AC

- **Eficiencia del POS/PCC**

Tiempos de procesamiento

El tiempo de procesamiento del POS y del PCC se muestra en las Figuras 39 y 40. El tiempo de inicialización del POS es significativamente mayor que el tiempo del PCC ya que al inicializarse realiza una conexión de prueba con el AC, que no se lleva a cabo al ejecutar la aplicación del PCC.

Hot Spots - Method	Self time [%]	Self time	Invocations
pos2.POS2View.**initComponents** ()		402 ms (58,2%)	1
pos2.POS2App.**startup** ()		222 ms (32,2%)	1
pos2.POS2App.**<init>** ()		33.7 ms (4,9%)	1
pos2.POS2View.**<init>** (org.jdesktop.application.SingleFrameApplication)		31.7 ms (4,6%)	1
pos2.POS2View.**run** ()		0.660 ms (0,1%)	1
pos2.POS2View$2.**<init>** (pos2.POS2View)		0.031 ms (0%)	1
pos2.POS2View$5.**<init>** (pos2.POS2View)		0.031 ms (0%)	1
pos2.POS2View$1.**<init>** (pos2.POS2View)		0.022 ms (0%)	1
pos2.POS2View$4.**<init>** (pos2.POS2View)		0.021 ms (0%)	1
pos2.POS2View$3.**<init>** (pos2.POS2View)		0.021 ms (0%)	1

Figura 39. Tiempo de procesamiento del PCC.

Hot Spots - Method	Self time [%]	Self time	Invocations
puntodeventa.PuntoDeVentaView.**<init>** (org.jdesktop.application.SingleFrameApplication)		2372 ms (78,2%)	1
puntodeventa.PuntoDeVentaView.**initComponents** ()		401 ms (13,2%)	1
puntodeventa.PuntoDeVentaApp.**startup** ()		233 ms (7,7%)	1
puntodeventa.PuntoDeVentaApp.**<init>** ()		25.3 ms (0,8%)	1
puntodeventa.PuntoDeVentaView.**conexionLector** ()		0.105 ms (0%)	1
puntodeventa.PuntoDeVentaView$2.**<init>** (puntodeventa.PuntoDeVentaView)		0.032 ms (0%)	1
puntodeventa.PuntoDeVentaView$8.**<init>** (puntodeventa.PuntoDeVentaView)		0.031 ms (0%)	1
puntodeventa.PuntoDeVentaView$7.**<init>** (puntodeventa.PuntoDeVentaView)		0.029 ms (0%)	1
puntodeventa.PuntoDeVentaView$4.**<init>** (puntodeventa.PuntoDeVentaView)		0.028 ms (0%)	1
puntodeventa.PuntoDeVentaView$3.**<init>** (puntodeventa.PuntoDeVentaView)		0.028 ms (0%)	1
puntodeventa.PuntoDeVentaView$5.**<init>** (puntodeventa.PuntoDeVentaView)		0.027 ms (0%)	1
puntodeventa.PuntoDeVentaView$6.**<init>** (puntodeventa.PuntoDeVentaView)		0.026 ms (0%)	1
puntodeventa.PuntoDeVentaView$1.**<init>** (puntodeventa.PuntoDeVentaView)		0.021 ms (0%)	1

Figura 40. Tiempo de procesamiento del POS

Consumo de Memoria

Tanto el PCC como el POS son clientes del servicio Web, por lo cual tienen poco procesamiento y consecuentemente bajo consumo de memoria como se observa en la Figura 41.

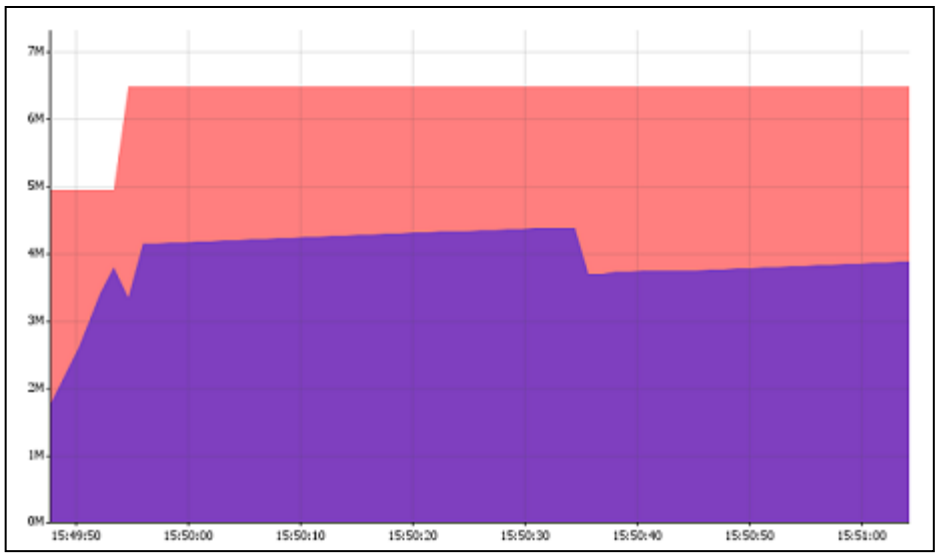


Figura 41. Consumo de memoria del POS

- ## Prueba de Estrés sobre el Servicio Web del AC

Es importante tener una idea del número de clientes que puede atender el servicio web de forma tal que el consumo de memoria sobre el servidor no mantenga bajo, menos de 100 Mb y el tiempo de respuesta en los puntos que acceden a él no excedan los 10 segundos por cada solicitud.

Se realizaron pruebas de consumo de memoria, variando la cantidad de clientes realizando solicitudes, los resultados obtenidos se condensan en las Figuras 42, 43 y 44.

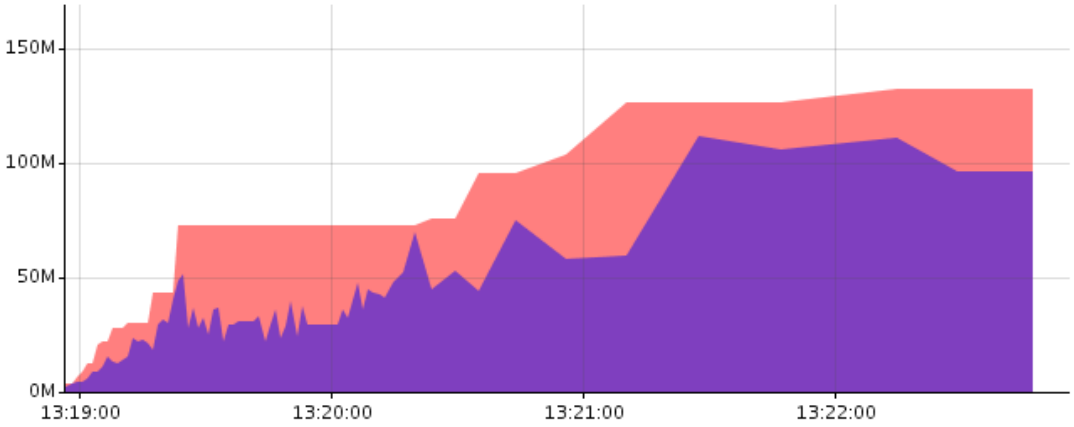


Figura 42. Consumo de memoria del AC de 75 clientes con 10 solicitudes c/u

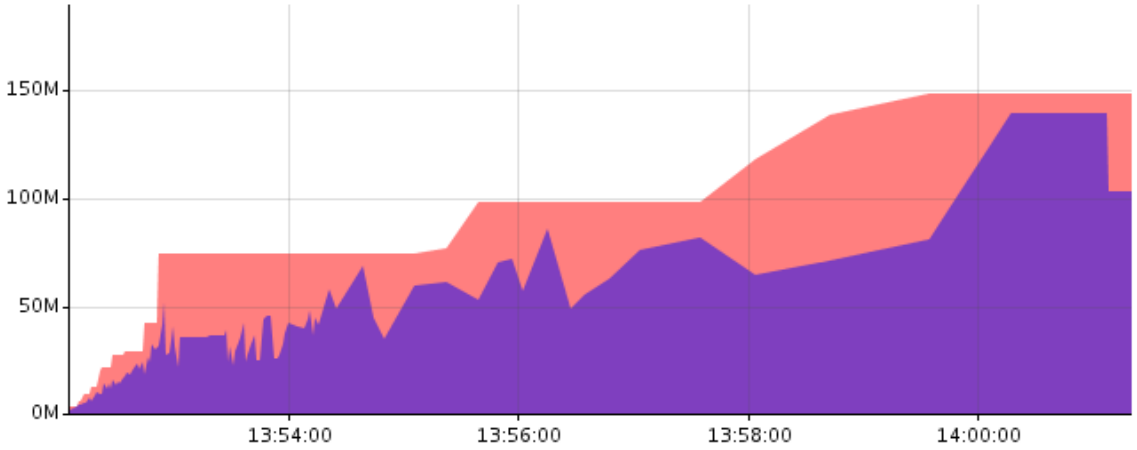


Figura 43. Consumo de memoria del AC de 100 clientes con 10 solicitudes c/u

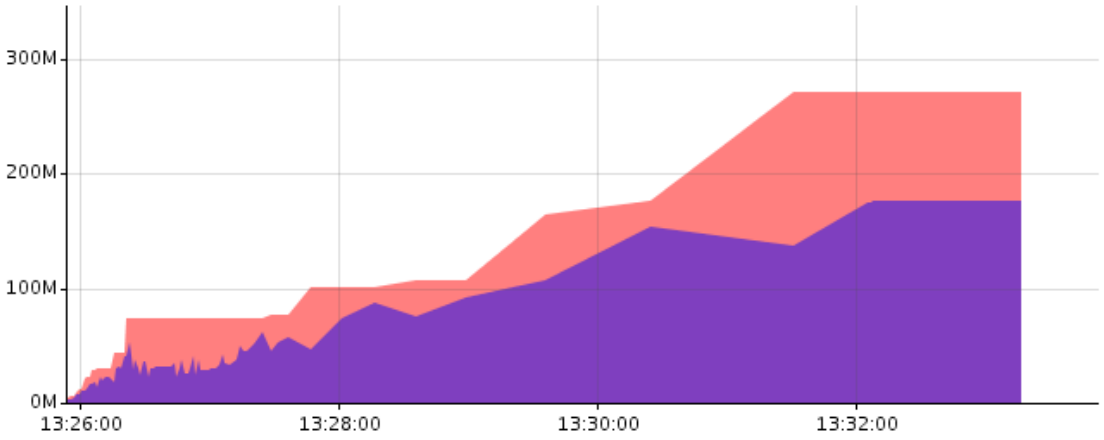


Figura 44. Consumo de memoria del AC de 125 clientes con 10 solicitudes c/u

El valor máximo de consumo de memoria para 75 clientes fue de 102 Mb, para 100 clientes fue de 140, y para 125 clientes fue de 183 Mb, en un equipo con procesador Pentium Core Duo de 1.86GHz y 1Gb de memoria RAM. Por lo cual se puede deducir que para más de 125 clientes el sistema comienza a congestionarse, claro que en un punto de creación de cuentas real hay un mayor intervalo de tiempo entre solicitudes de creación de cuenta haciendo que la carga sea menor que en la prueba de estrés.