

**ESCUELA POLITÉCNICA DEL EJÉRCITO
SEDE LATACUNGA**

CARRERA DE INGENIERIA SISTEMAS E INFORMÁTICA

**PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMAS E INFORMÁTICA**

**IMPLEMENTACIÓN DE LAS SEGURIDADES EN APLICACIONES
INALÁMBRICAS ORIENTADAS AL WEB: MÓDULO DE CARTERA DE
CLIENTES (CUENTAS POR COBRAR) SISTEMA ADMINISTRATIVO
INTEGRADO FENIX**

CHRISTIAN VINICIO CASTILLO GAVILANES

LATACUNGA – ECUADOR

2007

CERTIFICACIÓN

SE CERTIFICA QUE EL PRESENTE TRABAJO FUE DESARROLLADO POR CHRISTIAN VINICIO CASTILLO GAVILANES, BAJO NUESTRA SUPERVISIÓN.

ING. RAÚL ROSERO
DIRECTOR DE PROYECTO

ING. JAVIER MONTALUISA
CODIRECTOR DE PROYECTO

AGRADECIMIENTOS

MI MAS SINCERO AGRADECIMIENTO A DIOS, POR PERMITIRME ALCANZAR UN LOGRO MAS EN MI VIDA, A MIS PADRES, HERMANO, FAMILIARES POR COMPARTIR SU APOYO, AFECTO, EN ESPECIAL SIEMPRE SU AMOR QUE TUVIERON PRESENTE EN TODO MOMENTO.

EN ESPECIAL A MI PRIMO JUAN CARLOS QUE ME INCULCO QUE NUNCA ME RINDA Y QUE SIMPRE BUSQUE ALCANZAR MIS METAS QUE ME LAS E PLANTEADO.

A LA ESPE SEDE LATACUNGA, PROFESORES QUE BRINDARON SUS CONOCIMIENTOS A MIS AMIGOS, COMPAÑEROS POR COMPARTIR MOMENTOS DE ALEGRIA LOS CUALES GUARDARE POR SIEMPRE EN MI CORAZON.

CHRISTIAN.

PRESENTACIÓN

EL SIGUIENTE PROYECTO ESTA ORIENTADO HACIA LA NUEVA TECNOLOGÍA COMO LO ES LA TECNOLOGÍA WAP CON SUS SEGURIDADES CORRESPONDIENTES, UN TEMA MUY INTERESANTE E INDISPENSABLE EN EL CAMPO PROFESIONAL, Y DE GRAN AYUDA A ESTUDIANTES, PROFESIONALES SIRVIENDO COMO FUENTE DE CONSULTA.

ASI COMO TAMBIÉN SU CONFIGURACION VENTAJAS.

Latacunga, octubre del 2007.

Christian Vinicio Castillo Gavilanes
AUTOR

Ing. Edison Espinoza
CORDINADOR DE LA CARRERA DE INGENIERIA EN SISTEMAS E
INFORMÁTICA

Dr. Eduardo Vázquez Alcázar
SECRETERIA ACADEMICA ESPE-L

CAPÍTULO I

TECNOLOGÍA WAP Y SU FUNCIONAMIENTO

1.1 INTRODUCCIÓN.

WAP¹ define un conjunto de componentes estándar que permiten y hacen posible la comunicación entre distintas terminales móviles y servidores de red.

Cuando se habla de terminales móviles es importante que esto sea entendido tanto para el grupo de teléfonos como también el grupo de equipos portátiles, asistentes personales, etc.

Para ello en la evolución de las redes de telecomunicaciones se adoptado en una estrategia que es de dotar a los usuarios de “movilidad”, de tal manera que estos puedan establecer una comunicación segura, independiente y en tiempo real en el lugar que se encuentren.

Con la utilización de esta nueva tecnología el abonado o usuario podrá acceder a la compra de billetes de avión, gestión de cartera de valores y de una infinidad de aplicaciones, con sus respectivas desventajas y ventajas que aporta el teléfono móvil como media de navegación.

1.2 HISTORIA DE WAP.

La tecnología WAP nace a partir del año 1997 cuando Ericsson, Motorola, Nokia y Unwired Planet (hoy Phone.com/Openwave)² a fundar, el WAP Fórum ³ con el objetivo inicial de definir un conjunto de especificaciones para el desarrollo de aplicaciones para la industria de las telecomunicaciones inalámbricas.

La tecnología WAP es capaz de funcionar sobre cualquier dispositivo que disponga de conexión a una red inalámbrica (móvil, PDAs⁴, etc.).

Las especificaciones WAP definen un conjunto de protocolos que afectan el funcionamiento de las aplicaciones, las sesiones de conexión, las transacciones, la seguridad y los niveles de transporte, permitiendo a los operadores, fabricantes y desarrolladores de aplicaciones hacer frente a los

¹ WAP: Wireless Application Protocol o Protocolo de Aplicaciones Inalámbricas.

² Ericsson, Motorola, Nokia y Unwired Planet (hoy Phone.com/Openwave): empresas desarrolladoras de teléfonos móviles.

³ WAP Fórum: forum creado para el desarrollo de la Tecnología WAP.

⁴ PDAs: Siglas para Personal Digital Assistant o Asistente Personal Digital.

requerimientos de flexibilidad y diferenciación que cada vez más exige el mundo de las telecomunicaciones sin cable.

Las especificaciones desarrolladas para la versión WAP 1.0 no tuvieron resultados satisfactorios, y la mayoría de los fabricantes esperó la versión WAP 1.1 para ser disponible en terminales celulares con esa tecnología, siendo que los primeros terminales llegaron al mercado en mediados de 1999. La versión WAP 1.2.1 fue finalizada en Junio de 2000, y ya introducía nuevas funcionalidades, tales como la tecnología PUSH⁵. La versión actual, WAP 2.0, fue finalizada y disponible en enero de 2002.

WAP es un estándar global que no está controlado por ninguna compañía en solitario, lo que asegura su democracia, su apertura y su universalidad.

1.2.1 Evolución Del WAP.

La tecnología WAP como todas las cosas tiene su propia evolución:

1.2.1.1 Arquitectura WAP 1.X.

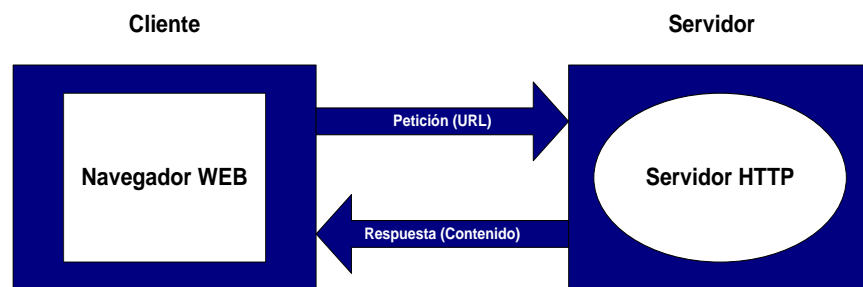


Figura 1.1: Arquitectura Web⁶.

⁵ Tecnología PUSH: Webcasting o Difusión en el Web.

⁶ Figura 1.1: Arquitectura Web por <http://www.cybercursos.net>.

Como se observa en la Figura 1.1 WAP esta basado en una arquitectura Web cliente-servidor, el cliente es un ordenador con un navegador Web que realiza peticiones HTTP⁷ al servidor, el cual se encarga en devolver las páginas solicitadas al ordenador.

La arquitectura WAP 1.x extiende la estructura Web introduciendo un elemento intermedio, el Proxy⁸ WAP, cuyas funciones más importantes incluyen la de traducción (Gateway⁹) entre los protocolos usados en Internet y el medio radio, además de poder ser utilizado como caché de páginas visitadas para que el rendimiento del sistema sea óptimo.

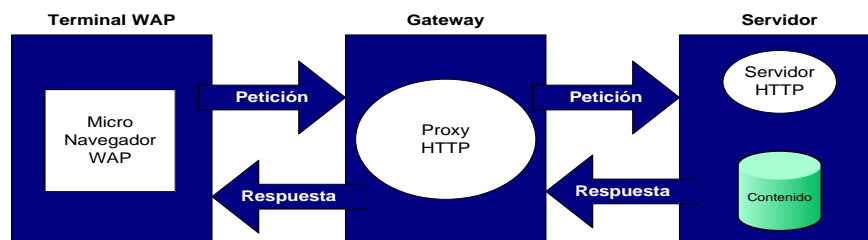


Figura 1.2: Arquitectura WAP¹⁰.

En la figura 1.2, el cliente es un terminal móvil con capacidad de navegación WAP que hace las peticiones de las páginas a un Proxy WAP, que es el encargado de traducirlas a peticiones HTTP, las cuales son enviadas al servidor Web que contiene la página solicitada.

El servidor devuelve la página al Proxy y éste la recodifica para ser enviada al cliente de una manera eficiente a través del medio radio.

⁷ HTTP: HyperText Transfer Protocol o Protocolo de Transferencia de Hipertexto, es el protocolo usado en cada transacción de la Web.

⁸ Proxy: es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

⁹ Gateway es un equipo que permite interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación.

¹⁰ Figura 1.2: Arquitectura WAP por <http://www.cybercursos.net>.

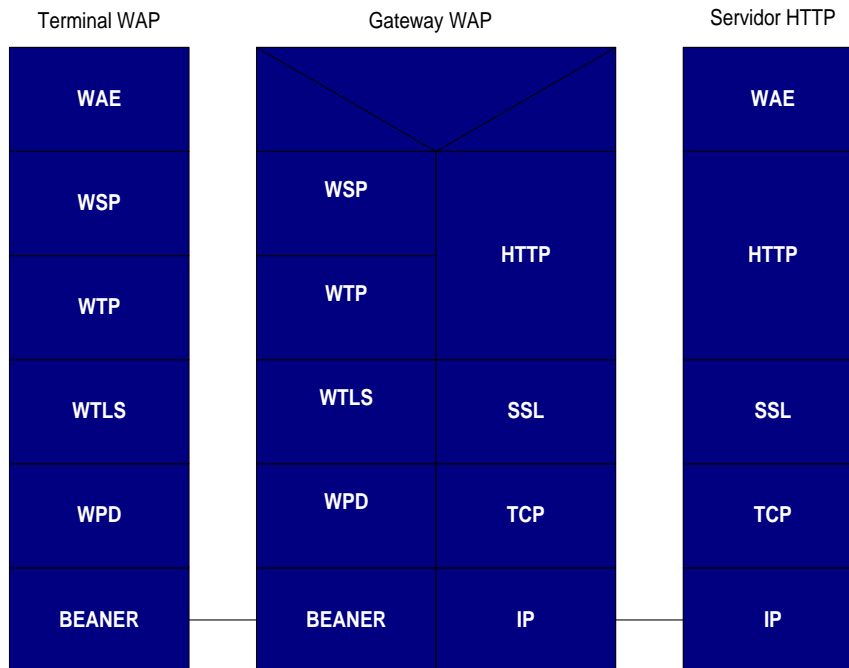


Figura 1.3: Torre de Protocolo WAP 1.x¹¹.

Como se explica en la figura 1.3 la torre de protocolo WAP 1.x esta conformada en tres partes fundamentales como son:

Servidor HTTP: esta conformada por los protocolos clásicos como son HTTP, SSL¹², TCP e IP¹³ más uno que es el WAE (Wireless Application Environment – Entorno de aplicación inalámbrica).

En este servidor las paginas Web que se deben publicar tienen que tener un formato específico basado en un **lenguaje de marcas inalámbricas** llamado **WML (Wireless Markup Language)** similar **HTML**¹⁴.

Terminal WAP: está conformada por las capas WAE (Wireless Application Environment – Entorno de aplicación inalámbrica), WSP (Wireless Session Protocol – Protocolo Inalámbrico de Sesión), WTP (Wireless Transaction Protocol – Protocolo Inalámbrico de Transacciones), WTLS (Wireless Transport Layer Security – Capa de Seguridad de Transporte Inalámbrico), WDP (Wireless Datagram Protocol – Protocolo Inalámbrico de Datagramas), BEANER (tecnología usada como portadora del servicio).

¹¹ Figura 1.3: Torre de Protocolo WAP 1.x por http://www.wikilearning.com/componentes_de_wap-wkccp-20821-5.htm

¹² SSL: Secure Sockets Layer son [protocolos criptográficos](#) que proporcionan comunicaciones [seguras](#) en [Internet](#).

¹³ TCP: (Transmission Control Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en [Internet](#) e IP: Protocolo de Internet un protocolo no orientado a la conexión, usado tanto por el origen como por el destino para la comunicación de estos a través de una red (Internet) de paquetes conmutados.

¹⁴ HTML: HyperText Markup Language o Lenguaje de Marcas Hipertextuales. Es un [lenguaje de marcación](#) diseñado para estructurar textos y presentarlos en forma de [hipertexto](#), que es el formato [estándar](#) de las [páginas web](#).

Gateway WAP: conformado en una forma compacta por la particularidad de todos los protocolos del servidor y las capas del terminal WAP, el cual nos permite interactuar de una pasarela a otra.

1.2.1.2 Arquitectura WAP 2.0.

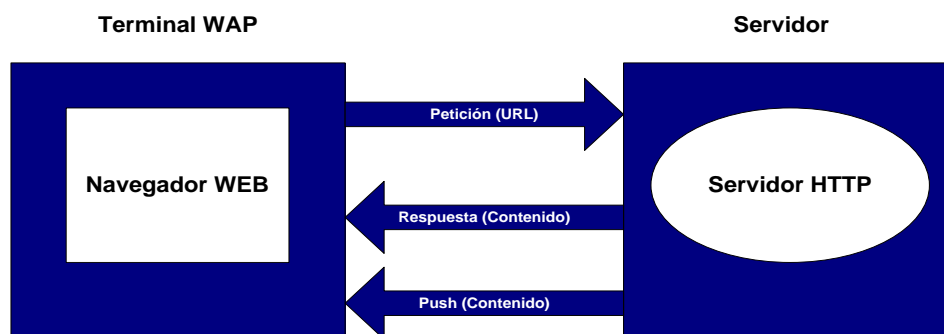


Figura 1.4: Arquitectura WAP 2.0¹⁵.

En la versión del protocolo WAP 2.0 (figura 1.4) se extiende la arquitectura de protocolos de forma que se asemeje a la arquitectura Web, pero con ciertas mejoras, como es el hecho de que sea el propio servidor el que pueda iniciar el envío de información sin que el cliente haya realizado ninguna petición (tecnología Push).

1.3 WIRELESS APPLICATION PROTOCOL (WAP).

WAP esta basado en los estándares de Internet (arquitectura definida para el World Wide Web (WWW)), que ha sido desarrollado para navegar en los teléfonos celulares a través de Internet.

¹⁵ Figura 1.4: Arquitectura WAP 2.0 por http://www.wikilearning.com/el_wap_forum-wkccp-20821-4.htm.

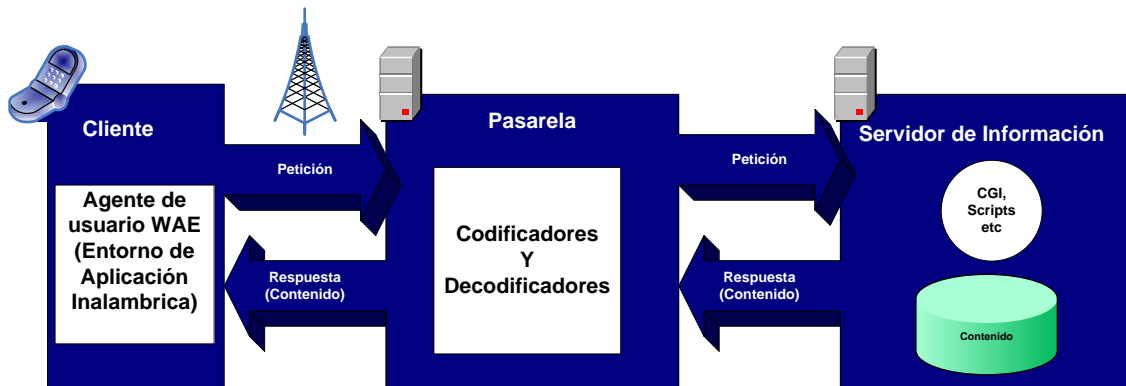


Figura 1.5: Modelo del funcionamiento del WAP¹⁶.

En el terminal inalámbrico (teléfono móvil) existiría un “micro navegador” encargado de la coordinación con la pasarela, a la cual la realiza peticiones de información que son adecuadamente tratadas y redirigidas al servidor de información adecuado.

Una vez procesada la petición de información en el servidor, se envía esta información a la pasarela que de nuevo procesa adecuadamente para enviarlo al terminal inalámbrico.

Para conseguir consistencia en la comunicación entre el terminal móvil y los servidores de red que proporcionan la información, WAP define un conjunto de componentes estándar:

- Un modelo de nombres estándar. Se utilizan las URL¹⁷ definidas en WWW para identificar los recursos locales del dispositivo (tales como funciones de control de llamada) y las URL (también definidas en el WWW) para identificar el contenido WAP en los servidores de información.
- Un formato de contenido estándar, basado en la tecnología WWW.
- Unos protocolos de comunicación estándares, que permitan la comunicación del micro navegador del terminal móvil con el servidor Web en red.

¹⁶Figura 1.5: Modelo del funcionamiento del WAP por <http://www.cybercursos.net>.

¹⁷ URL: permite la inclusión de pequeños elementos de datos en línea, como si fueran referenciados hacia una fuente externa.

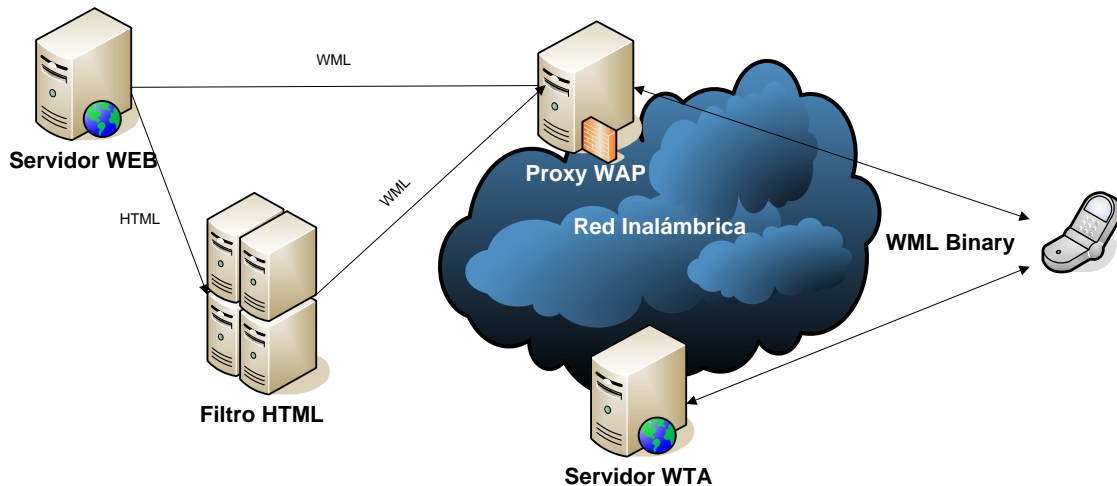


Figura 1.6: Ejemplo de una Red WAP¹⁸.

En el ejemplo de la figura 1.6, nuestro terminal móvil tiene dos posibilidades de conexión: a un Proxy WAP, o a un servidor WTA.

- El Proxy WAP traduce las peticiones WAP a peticiones Web, de forma que el cliente WAP (el teléfono móvil) pueda realizar peticiones de información al servidor Web. Adicionalmente, codifica las respuestas del servidor Web en un formato binario compacto, que es interpretable por el cliente.
- El Servidor WTA está pensado para proporcionar acceso WAP a las facilidades proporcionadas por la infraestructura de telecomunicaciones del proveedor de conexiones de red.
- La tecnología tiene como premisas iniciales el uso de estándares abiertos ya existentes (como los protocolos HTTP, o el XML¹⁹), la independencia de la tecnología de comunicaciones móviles sobre la que se implemente y la independencia del terminal móvil.

Las especificaciones WAP surgen a partir de la adopción de la tecnología Internet a las restricciones del sistema inalámbrico.

Las características clave que presenta WAP son las siguientes:

¹⁸ Figura 1.6: Ejemplo de una Red WAP por <http://www.cybercursos.net>.

¹⁹ XML: eXtensible Markup Language o [lenguaje de marcas](#) extensible, es un [metalenguaje](#) extensible de etiquetas desarrollado por el [World Wide Web Consortium](#).

- Un modelo de programación similar al de Internet como los navegadores Web, los dispositivos WAP se basan en una serie de transacciones pregunta/respuesta con los servidores de contenidos.
- Wireless Markup Language (WML).
- Wireless markup Language Script (WMLScript).
- Especificación de un micro navegador define como deben ser interpretados y presentados al usuario los lenguajes WML y el WMLScript.
- Marco para WTA (Wireless Telephony Application) proporciona finalidades que las operadoras telefónicas pueden utilizar para integrar funciones de telefonía en el navegador.

1.4 COMPONENTES DE LA ARQUITECTURA WAP.

La arquitectura WAP está pensada para proporcionar un "entorno escalable y extensible para el desarrollo de aplicaciones en dispositivos de comunicación móvil". Para esto, define una estructura en capas, en la cual cada capa es accesible por la capa superior así como por otros servicios y aplicaciones a través de un conjunto de interfaces muy bien definidos y especificados.

Las capas de la arquitectura WAP se acopian en el siguiente diagrama:

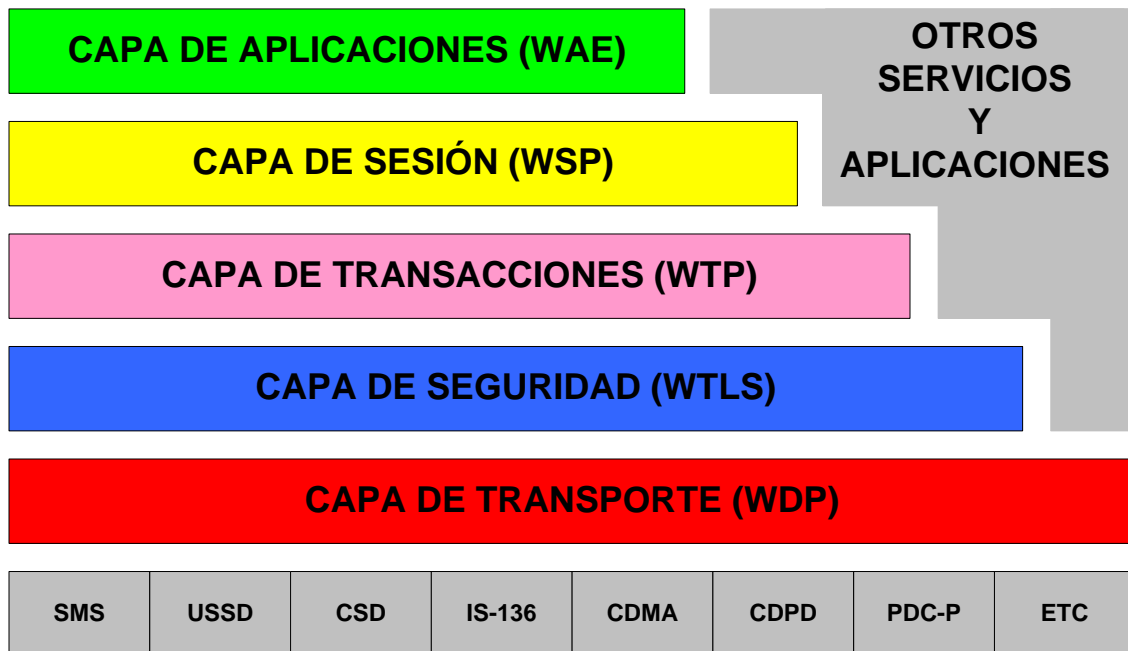


Figura1.7: Arquitectura WAP²⁰.

1.5 CAPA DE APLICACIÓN (WAE).

Wireless Application Environment (WAE), esta basado en la combinación de World Wide Web (WWW) y la tecnología de Comunicaciones Móviles, su objetivo es proporcionar un entorno inter operable para desarrollar aplicaciones en diferentes plataformas.

Esta capa contiene el micro navegador y es donde se especifica los lenguajes de programación Wireless Markup Language (WML) y WMLScript, incluyendo las funcionalidades de WTA y WTAI para servicios telefónicos.

1.5.1 Wireless Markup Language (WML).

Es un lenguaje de marcas basado en XML (Extensible Markup Language) y diseñado para crear aplicaciones WAP independientes del dispositivo utilizado, y posee las siguientes características:

²⁰ Figura1.7: Arquitectura WAP por <http://www2.uah.es/vivatacademia/ficheros/n54/wap.pdf>.

- **Baraja de Cartas:** mientras el objeto HTML más común es una página, el WML usa el concepto de una baraja de cartas ("deck-of-cards"). Cuando el usuario solicita un objeto WML él recibe ese conjunto de cartas y navega por ellas en el navegador del terminal móvil.
- **Texto e Imágenes:** tiene soporte limitado para layout y frame, siendo más adecuada para la presentación de textos e imágenes en el terminal móvil.
- **Aplicaciones de Servidor:** así como el HTML, es posible escribir scripts y aplicaciones para ejecutar en el servidor, con el objetivo de generar páginas dinámicas.
- **Imágenes:** el soporte a imágenes todavía es limitado. La conversión de los formatos usuales de Internet para el formato WML es hecha en el gateway WAP.
- **Eventos, Variables y Estados:** tiene soporte para el tratamiento de eventos y timers, y aún da soporte a la manutención de variables y estados durante sesiones activas independiente de la calidad del señal de la red.
- **Formato Binario:** aunque el formato de las páginas HTML y WML sea texto, el gateway WAP compila el objeto y genera un formato binario para ser enviado para el navegador del terminal móvil.

1.5.2 Wireless markup Language Script (WMLScript).

Es un lenguaje de scripting basado en el ECMAScript²¹ y que tiene por objetivo extender las funcionalidades del WML, la diferencia con el WML es que se basa en lo que el usuario ve y el WMLScript tiene muy pocas capacidades de interfaz con el usuario.

Este está diseñado para agregar procedimientos lógicos y capacidades computacionales robustas a WML.

1.5.3 Wireless Telephony Applications (WTA).

Es un entorno para aplicaciones y servicios de telefonía, con el objetivo de suministrar una interfase entre el contenido WAP y las funcionalidades normales de un terminal móvil.

²¹ ECMAScript es una especificación de [lenguaje de programación](#) publicada por [ECMA International](#).

1.5.4 Wireless Telephony Application Interface (WTAI).

Es una interfaz utilizada en los terminales móviles para operaciones locales de control de llamadas (recepción, iniciación y terminación) y acceso a listines telefónicos.

1.6 CAPA DE SESIÓN (WSP).

Wireless Session Protocol (WSP), permite al WAP definir sesiones y conexiones que consideren el estado de la parte cliente del terminal móvil.

La existencia del WSP facilita el soporte a la tecnología PUSH, donde los servidores envían de forma espontánea informaciones solicitadas por los usuarios.

El WSP ofrece 2 tipos de servicios:

- **Servicio orientado a la conexión:** es el más confiable y garantiza el envío de mensajes para el destino solicitado.
- **Servicio no orientado a conexión:** usa la misma filosofía “envíe y olvide” del UDP del protocolo IP, pero el encabezamiento de los mensajes es más complejo pues debe incluir la información suficiente para que ellos sean correctamente enviados a su destino.

Esta capa proporciona las siguientes funcionalidades:

- Establecimiento y liberación de conexiones entre cliente y servidor.
- Intercambio de información entre cliente y servidor.
- Negociación de las características del protocolo.
- Suspensión y reanudación de la sesión.

1.7 CAPA DE TRANSACCIONES (WTP).

Wireless Transaction Protocol (WTP), fue desarrollado para ser más confiable que el UDP²², sin embargo menos pesado y complejo que el TCP del protocolo IP.

El WTP es un protocolo orientado a mensajes, al contrario del HTTP/TCP, que es orientado a paquetes.

Busca garantizar que un mensaje sea entregado, o sea, que la transacción fue completada, mientras el HTTP/TCP busca garantizar que un conjunto de paquetes sea entregado en orden correcta.

WTP proporciona los servicios necesarios para soportar las transacciones y pueden ser:

- Peticiones inseguras de un solo camino.
- Peticiones seguras de un solo camino.
- Transacciones seguras de dos caminos.

1.8 CAPA DE SEGURIDAD (WTLS).

(Wireless Transport Layer Security), es un protocolo basado en el estándar SSL, utilizado en el entorno Web, para la seguridad en la transferencia de datos, está proporciona a las capas de niveles superiores de WAP una interfaz de servicio de transporte seguro, que lo resguarde de una interfaz de transporte inferior.

Las funcionalidades de esta capa son las siguientes:

- **Integridad de los datos:** se asegura que la información intercambiada entre el terminal y el servidor de aplicaciones, no haya sido modificada.

²² UDP User Datagram Protocol (UDP) es un [protocolo](#) del [nivel de transporte](#) basado en el intercambio de [datagramas](#).

- **Privacidad de los datos:** se asegura que la información intercambiada entre el terminal y el servidor de aplicaciones, no pueda ser captada ni entendida por elementos externos a la comunicación.
- **Autenticación:** se ofrecen servicios para determinar la autenticidad del terminal y del servidor de aplicaciones.

1.9 CAPA DE TRANSPORTE (WDP).

Wireless Datagram Protocol (WDP), está dividida entre el WTP y el WDP.

El WDP sirve de interfase entre cualquier red de transporte (IS-95, GSM, GPRS²³, etc.) y las capas superiores del WAP.

Con el objetivo de usar componentes existentes en las recomendaciones de los protocolos de Internet, el WAP usa el UDP siempre que una red de transporte soporte el protocolo IP.

El UDP es un protocolo de entrega de paquetes, que no hace el reenvío de paquetes perdidos o con atraso.

El WAP tampoco controla la segmentación de paquetes inherente al TCP/IP.

En el seguimiento WAP los paquetes tienen tamaño fijo, y cabe al TCP definir el tamaño de fragmentación de paquetes, caso sea necesario, en el seguimiento Internet de la red.

Adicionalmente, el WDP controla el número de la puerta para las aplicaciones, de forma a permitir que varias aplicaciones puedan ser ejecutadas en el mismo terminal.

1.10 EL ENTORNO INALÁMBRICO DE APLICACIONES.

El objetivo del Entorno Inalámbrico de Aplicaciones es construir un entorno de aplicación de propósito general, basado fundamentalmente en la filosofía y tecnología del World Wide Web (WWW).

²³ IS-95, GSM, GPRS: estándares de telefonía móvil celular.

La arquitectura del Entorno Inalámbrico de Aplicaciones (WAE) está enfocado principalmente sobre los aspectos del cliente de la arquitectura del sistema de WAP, se debe a que la parte que más interesa de la arquitectura es aquella que afecta principalmente a los terminales móviles.

Entre los agentes de usuario localizados en el cliente (en el terminal móvil) y los servidores de información se define un nuevo elemento:

Las pasarelas, su función es codificar y decodificar la información intercambiada con el cliente, para así minimizar la cantidad de datos radiados, así como minimizar el proceso de la información por parte del cliente.



Figura 1.8: Componentes del Cliente WAE²⁴.

Como se observa en la figura 1.8 WAE se divide en dos capas lógicas:

- **Los agentes usuarios:** que incluyen los navegadores, agenda, etc.
- **Servicios y formatos:** que incluyen el conjunto de elementos y formas accesibles por los agentes de usuario como son el WML, WMLScript, formatos de imágenes, etc.

²⁴ Figura 1.8: Componentes del Cliente WAE por <http://www2.uah.es/vivatacademia/ficheros/n54/wap.pdf>.

Dentro de WAE se separan Servicios de Agentes de Usuario, lo que proporciona flexibilidad para combinar varios Servicios dentro de un único agente de usuario, o para distribuir los servicios entre varios agentes de usuario.

Los dos agentes de usuario más importantes son el WML y el WTA.

El agente de usuario para WML es fundamental en la arquitectura del Entorno Inalámbrico de Aplicación, este agente de usuario no está definido formalmente dentro de esta arquitectura, ya que sus características y capacidades se dejan en manos de los encargados de su implementación.

1.11 EL PROTOCOLO INALÁMBRICO DE SESIÓN.

El Protocolo Inalámbrico de Sesión cumple las siguientes funciones:

- Establecer una conexión fiable entre el cliente y el servidor.
- Liberar esta conexión de una forma ordenada.
- Ponerse de acuerdo en un nivel común de funcionalidades del protocolo, a través de la negociación de las posibilidades.
- Intercambiar contenido entre el cliente y el servidor utilizando codificación compacta.
- Suspender y recuperar la sesión.

Este protocolo ha sido definido únicamente para el caso de la navegación, llamado WSP/B12, esta implementación está realizada para el establecimiento de una conexión sobre la base de un protocolo compatible con HTTP1.1, de esta forma, se define un conjunto de primitivas de servicios para permitir la comunicación entre el equipo cliente y el equipo servidor.

Primitivas de Sesión.

- **S-Connect:** se utiliza para inicializar la conexión, y para la notificación de su éxito.
- **S-Disconnect:** se utiliza para desconectar una sesión y notificar al usuario.

- **S-Suspend:** se utiliza para suspender una sesión, o no se puede establecer.
- **S-Resume:** se utiliza para solicitar recuperar una sesión.
- **S-Exception:** se utiliza para notificar aquellos eventos que no están asignados a una transacción en particular.
- **S-MethodInvoke:** se utiliza para solicitar una operación que debe ser ejecutada en el servidor.
- **S-MethodResult:** se utiliza para devolver una respuesta a una petición de operación.
- **S-MethodAbort:** se utiliza para abortar una solicitud de ejecución de operación.
- **S-Push:** se utiliza para enviar información no solicitada desde el servidor.
- **S-ConfirmedPush:** realiza las mismas funciones que la anterior pero con confirmación.
- **S-PushAbort:** se utiliza para anular una primitiva anterior de tipo S-Push o S-ConfirmedPush.

Primitivas de Servicio.

- **Request (red):** se utiliza cuando una capa superior solicita un servicio de la capa inmediatamente inferior.
- **Indication (ind):** una capa solicita un servicio utiliza para notificar a la capa superior de las actividades relacionadas con su par, o con el proveedor.
- **Response (res):** se utiliza para reconocer la recepción de la primitiva de tipo Indication.
- **Confirm (cnf):** _capa que proporciona el servicio requerido utiliza esta primitiva para modificar que la actividad ha sido satisfactoriamente.

1.12 EL PROTOCOLO INALÁMBRICO DE TRANSACCIÓN.

El Protocolo Inalámbrico de Transacción proporciona los servicios necesarios que soporten aplicaciones de “navegación” (del tipo petición/respuesta).

Las características de este protocolo son:

- Proporciona tres clases de servicios de transacción:

Clase 0: mensaje de solicitud no seguro, sin mensaje de resultado.

Clase 1: mensaje de solicitud seguro, sin mensaje de resultado.

Clase 2: mensaje de solicitud seguro, con un mensaje de resultado seguro.

- Seguridad opcional usuario a usuario.
- Puede contener algún tipo de información adicional relacionada con la transacción, como medidas de prestaciones, etc.
- Se proporcionan mecanismos para minimizar el número de transacciones que se reenvían como resultado de paquetes duplicados.
- Se permiten las transacciones asíncronas.
- Transferencia de Mensajes.

Dentro de este protocolo se distinguen dos tipos de mensajes:

Los mensajes de datos transportan únicamente datos de usuario.

Los mensajes de control se utilizan para los asentimientos, informes de error, etc. pero sin transportar datos de usuario.

- Retransmisión hasta el asentimiento.
- Asentimiento de usuario.
- Información en el último asentimiento.
- Concatenación y Separación.
- Transacciones Asíncronas.

- Identificador de la Transacción.
- Segmentación y re-ensamblado (opcional).

Crea un conjunto de primitivas tales como:

Primitivas de Servicio de Transacción.

- **TR-Invoke:** se utiliza para hincar una nueva transacción.
- **TR-Result:** se utiliza para devolver el resultado de transacción iniciada.
- **TR-Abort:** se utiliza par abortar una transacción existente.

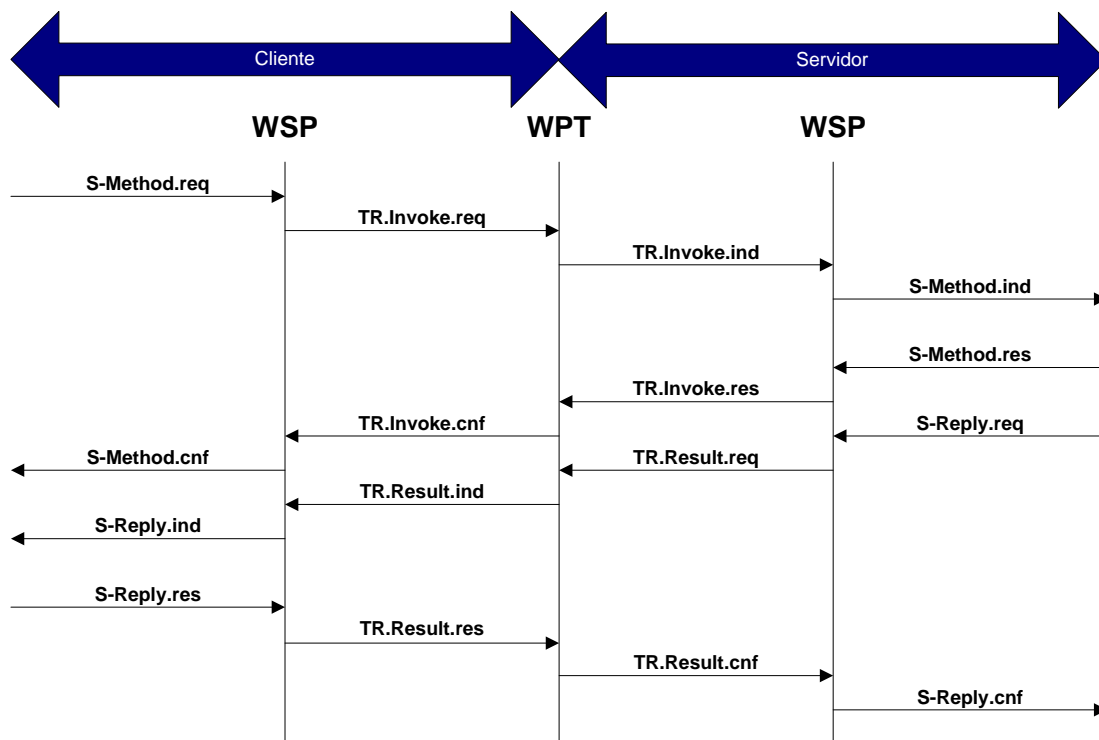


Figura 1.9: Ejemplo de Intercambio de Primitivas de Capa de Sesión y Transacción²⁵.

En la figura 1.9 se muestra como funciona las primitivas de la capa de sesión y transacción.

²⁵ Figura 1.9: Ejemplo de Intercambio de Primitivas de Capa de Sesión y Transacción por <http://www2.uah.es/vivatacademia/ficheros/n54/wap.pdf>.

1.13 EL PROTOCOLO INALÁMBRICA DE SEGURIDAD DE TRANSPORTE.

El Protocolo Inalámbrica de Seguridad de Transporte (WTLS), compone una capa modular, que depende del nivel de seguridad requerido por una aplicación, proporciona a las capas de nivel superior de WAP de una interfaz de servicio de transporte seguro.

Este protocolo consta de primitivas tales como:

Servicio de Capa de Seguridad.

- **SEC-Unitdata:** se utiliza para intercambiar datos de usuario entre los dos participantes.
- **SEC-Create:** se utiliza para iniciar el establecimiento de una conexión segura.
- **SEC-Exchange:** se utiliza en la creación de una conexión segura si el servidor desea utilizar autenticación de clave pública o intercambio de claves con el cliente.
- **SEC-Commit:** se inicia cuando el handshaker se completa y cualquiera de los equipos participantes solicita cambiar a un nuevo estado.
- **SEC-Terminate:** se utiliza para finalizar la conexión.
- **SEC-Exception:** se utiliza para informar al otro extremo sobre las alertas de nivel de aviso.
- **SEC-Create-Request:** se utiliza por el servidor para solicitar al cliente que inicie un nuevo handshaker.

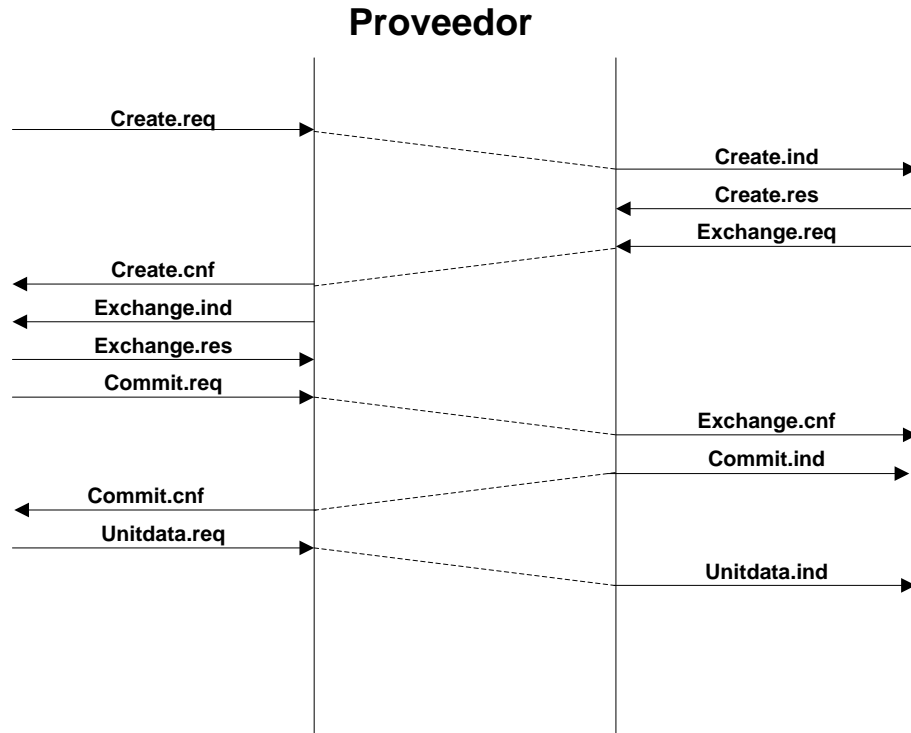


Figura 1.10: Secuencia de Primitivas para el establecimiento de una sesión segura²⁶.

La figura 1.10 nos muestra el intercambio de las primitivas cliente y servidor.

1.14 EL PROTOCOLO INALÁMBRICO DE DATAGRAMAS.

El Protocolo Inalámbrico de Datagramas (WDP) ofrece un servicio consistente al protocolo (Seguridad, Transacción y Sesión) de la capa superior de WAP, comunicándose de forma transparente sobre uno de los servicios portadores disponibles.

Este protocolo ofrece servicios a los protocolos superiores del estilo a direccionamiento por número de puerto, segmentación y re-ensamblado opcional y detección de errores opcional, de forma que se permite a las aplicaciones de usuario funcionar de forma transparente sobre distintos servicios portadores disponibles.

Este protocolo también consta de primitivas tales como:

²⁶ Figura 1.10: Secuencia de Primitivas para el establecimiento de una sesión segura por <http://www2.uah.es/vivatacademia/ficheros/n54/wap.pdf>.

Servicio de Capa de Datagramas

- **T-DUnidata:** es la utilizada para transmitir datos como datagramas, no requiere que exista una conexión para establecer.
- **T-DError:** se utiliza para proporcionar información a la capa superior cuando ocurre un error que pueda influenciar en el servicio requerido.

CAPÍTULO I I

SEGURIDADES.

2.1 INTRODUCCIÓN.

“La seguridad no es un producto, sino un proceso.” por Bruce Schneier²⁷.

Toda seguridad se trata de implementar un sistema robusto que a más de contar con medidas de seguridad como criptografía, etc. trabajen en conjunto.

En este capítulo se estudia los principales conceptos de seguridad, que van desde la determinación de la vulnerabilidad hasta la definición de mecanismos de criptografía, es por eso que las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social, por consiguiente la seguridad es primordial hoy en día en todo tipo de empresas para incrementar su desarrollo.

2.2 SEGURIDADES.

La seguridad es el conjunto de procedimientos y actuaciones en caminados a conseguir la garantía que funcione el sistema de información, obteniendo eficacia, integridad y alertando la detección de actividad ajena.

Por este motivo se subdivide en dos áreas fundamentales para obtener una seguridad más entendible.

Hardware: esta comprendida por:

- **Servidor:** llamados centro de proceso de datos.
- **Cliente:** son entendidos como aquellos equipos remotos que interactúan entre si con los servidores.
- **Líneas De Comunicación:** es una segmentación de red por cual transcurre la información deseada.

Software: esta comprendida por:

- **Sistema Operativo:** es el sistema de información con la base del funcionamiento lógico del mismo.

²⁷ Bruce Schneier (nacido el [15 de enero, 1963](#)) es un [criptógrafo](#), experto en [seguridad informática](#), y [escritor](#).

- **Base De Datos:** es un conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora.
- **Aplicaciones:** fue diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.

Para entender de seguridad existente tenemos que entender lo que es el CID²⁸.

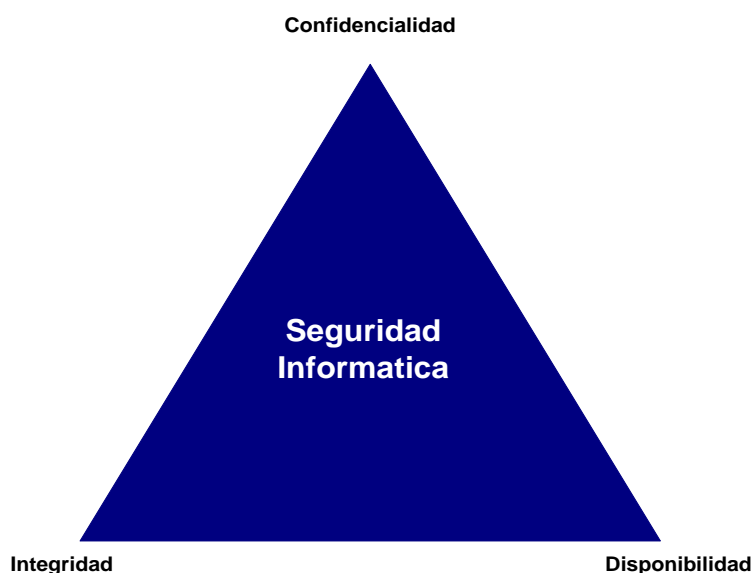


Figura 2.1: Principio Fundamentales De La Seguridad²⁹.

2.2.1 Confidencialidad.

Consiste en garantizar que los datos, objetos y recursos solamente puedan ser leídos por su dueño. Estos se encuentran almacenados en algún tipo de soporte físico (memoria, disco duro, disquetes, CD-ROM, etc.) o bien se encuentran en tránsito entre dos equipos a través de una red de comunicación.

Entre los ataques más frecuentes se puede citar los siguientes:

- **Los Sniffers De Red:** estos sniffers³⁰ capturan todo el tráfico por una red, la información no se encuentra cifrada y será conocida por el atacante.

²⁸ CID: Confidencialidad, Integridad, Disponibilidad.

²⁹ Figura 2.1 Principio Fundamentales De La Seguridad por Seguridad Informática Para Empresas Y Particulares Mc. Graw Hill.

- **El Acceso No Autorizado A Archivos:** esto se da cuando no existe o está mal configurado el control de acceso de los recursos, esto implica que personas no autorizadas accedan a la información.
- **El Acceso Remoto No Autorizado A Bases De Datos:** los ataques explotan errores de configuración en el control de acceso. El resultado final es el acceso indiscriminado a la información confidencial almacenada en la misma.

Las contramedidas para la confidencialidad frente a estas amenazas.

- **Cifrado De Datos:** garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados.

Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado llamado clave de cifrado.

- **Autenticación De Usuario:** asegura la identificación de los sujetos en una comunicación o sesión de trabajo, mediante contraseñas, la biometría, tarjetas inteligentes, etc.
Los datos almacenados en un equipo no siempre se encuentran cifrados, la autenticación se introduce en la sesión o autentica al usuario mediante una clave cifrada.
- **Autorización De Usuario:** una vez que la identidad del sujeto ha sido correctamente verificada, debe dotarse de privilegios para poder efectuar ciertas operaciones con los datos.
- **Clasificación De Datos:** la clasificación de datos ayuda a determinar cuánto esfuerzo, dinero y recursos deben destinarse para proteger los diferentes tipos de datos y controlar su acceso.

2.2.2 Integridad.

Consiste en garantizar que los datos, objetos y recursos no han sido alterados, permanecen completos y son fiables.

La integridad puede examinarse desde tres enfoques diferentes.

³⁰ Sniffers: es un programa de captura de las tramas de [red](#). Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

- Los sujetos no autorizados no deberían poder modificar la información en absoluto.
- Los sujetos autorizados no deberían poder realizar modificaciones no autorizadas.
- Los objetos deberían ser interna y externamente consistentes de manera que sus datos son correctos y verdaderos en todo momento.

2.2.3 Disponibilidad.

Consiste en garantizar que los datos permanecen accesibles sin interrupción cuando y en donde los necesiten.

No hay que olvidar interrupciones deliberadas del servicio como:

- **Ataques De Denegación De Servicio:** consiste en consumir todos los recursos del sistema objetivo de manera que no puede dar respuesta a las peticiones de usuarios legibles.
- **Destrucción De Archivos:** esto se da más por la introducción de virus, los cuales se infiltran y destruyen información necesaria por los usuarios.
- **Cortes En Las Líneas De Comunicación:** se trata de una forma sencilla de interrumpir la operación de una empresa en particular, cortando su vía de comunicaciones con el exterior.

2.3 PROBLEMAS DE SEGURIDAD.

Los problemas de la seguridad a nivel informático y de tecnología WAP se han clasificado de la siguiente manera por motivos particulares en esencia por los ladrones informáticos o personas no deseadas.

2.3.1 Problemas De Disponibilidad.

Es causada por errores de hardware o software que hacen perder archivos, información necesaria para la empresa.

Para poder luchar con este problema de disponibilidad al usuario se le crea una cultura de copia de seguridad en algún dispositivo de almacenamiento físico.

2.3.2 Problemas De Privacidad.

Los ordenadores domésticos son compartidos por varios usuarios, por lo que resulta frecuente que personas no deseadas accedan a la información de la empresa, para esto existe métodos como por ejemplo claves y otras seguridades.

2.3.3 Problemas Técnicos.

El **CLONING** es uno de los problemas muy particulares encargados por los operadores de la red, este consiste en la programación ilegal de los dispositivos móviles con una serie de combinaciones validas de acceso al servicio de comunicación de la red.

El **RECHIPPING** quiere decir una reidentificación que el operador de red toma como un abonado valido, que recibirá facturas por el servicio.

Los generadores de problemas obtienen Números de Serie Electrónicos (ESNs) por medio de examinadores de señal o clonación de dispositivos móviles.

El GSM previene el **CLONING**, al incorporar aspectos de seguridad como es la adición de un proceso de autenticación, cifrado, e identidad del abonado. En este proceso los números de serie son cifrados y el escaneo o monitoreo de señal se vuelve inútil.

2.3.4 Problema De Suscripción.

El problema de suscripción seda por la ambición o mira de ganar mercado rápidamente, en algunas ocasiones el proveedor del servicio no realiza apropiadamente la identificación y la revisión de crédito,

debido que el abonado hace uso de un tiempo libre de funcionamiento que no se ve reflejado en la facturación del servicio al abonado, provocando así una facturación menor por el servicio.

El problema de **ROAMING** o mejor dicho de itinerancia es otro tipo de fraude, este con solo la tarjeta SIM, el suscriptor se mueve a otra red, que tiene un acuerdo de **ROAMING** con la red de su localidad y hace uso del servicio incrementando su facturación, por su puesto sin la mínima intención de pagar.

Este fraude se ataca pro el método llamado **CALL-SELL** (al que llama vende), este es usado en muchas partes del mundo.

2.3.5 Problemas Internos.

Estos son problemas provocados por empleados que trabajan dentro de las empresas que proveen el servicio telefónico móvil, son reconexiones del servicio ilegal, un acceso no autorizado al mismo, mal uso de los esquemas proporcionales, un avanzada activación del SIM³¹, etc.

Para protegerse de los teléfonos clones existen dos técnicas:

- **Perfiles:** esta usa llamadas gravadas desde el interruptor móvil, crea y usa un perfil para cada abonado de forma individual, diferentes algoritmos supervisan el uso del abonado y se enfocan en el tiempo de llamada, localidad, limites del crédito, y el patrón de llamadas.
- **Firma Digital En Radio Frecuencias (RF):** con la ayuda de un equipo adicional a cada sitio de las celdas, las radios frecuencias hacen una buena pareja junto con la firma digital de RF para un teléfono individual, ya que estos son buenos parámetros para una base de datos, así poder denegar el acceso a lo teléfonos ilegales o clones.

2.3.6 Recomendaciones Al Abonado.

No dejar que cualquier persona utilice su teléfono a menos que este presente.

Permita que solamente los técnicos certificados de su compañía de servicio celular, instalen o prueben su teléfono.

³¹ SIM: Subscriber Identity Module, 'Módulo de Identificación del Suscriptor, es una [tarjeta inteligente](#) desmontable usada en [teléfonos móviles](#) que almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red, de forma que sea posible cambiar la línea de un terminal a otro simplemente cambiando la tarjeta.

No dejar a vista su teléfono en lugares no seguros etc.

Reporte a su compañía que provee el servicio, si recibe con mucha frecuencia llamadas de números equivocados o llamadas en las cuales cuelguen, estos eventos pueden indicar que su teléfono está clonado.

Controlar si hay actividad inusual o inesperada de llamadas en su cuenta mensual del teléfono.

Si encuentra fraude, la compañía celular coopere con el abonado con respecto a:

- Un cambio de número.
- Preparar las declaraciones juradas de las pérdidas por el fraude que han ocurrido en su número del teléfono móvil.

2.4 TIPOS DE SEGURIDADES Y SU FUNCIONAMIENTO.

2.4.1 Servicios De Seguridad.

Para proteger las comunicaciones es necesario dotarlas de estos servicios.

2.4.1.1 Autenticación De La Entidad Par.

Mediante este servicio se verifica la fuente de los datos. La autenticación puede ser de la entidad origen, de la entidad destino o de ambas a la vez. Los mecanismos de autenticación son:

- **Contraseña Y Respuesta:** se basa en la premisa de que sólo el usuario conoce la contraseña. Este sistema es más apropiado cuando la otra parte es una persona. Se usan principalmente dos protocolos: PAP³² y CHAP³³.
- **Certificados Digitales:** constituyen los fundamentos de dos importantes características de seguridad “autenticación y cifrado”.

El propósito de los certificados digitales es la autenticación del cliente, del servidor, firma de código, correo electrónico seguro, recuperación de archivos.

Las entidades que prestan el servicio son:

- GlobalSign.
- Thawte.
- VeriSign.

Se usa cuando no es suficiente la verificación del nombre de usuario en el otro extremo y se hace necesaria una autenticación de la máquina, a través de la cual está interactuando el usuario con el sistema. Son emitidos por una autoridad certificadora y tienen validez para autenticar tanto a clientes como a servidores mediante una clave pública.

Existen varias clases de certificados tales como:

- **Certificados De Servidor:** aporta a un WEB SITE³⁴ la característica de seguridad y confianza necesaria para poder entablar cualquier tipo de relación con los potenciales usuarios.

Permite incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web.

Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta, passwords, etc., cobra especial importancia dentro del área del comercio electrónico, donde la seguridad de los datos es la principal barrera para el desarrollo de los sistema.

³² PAP (Password Authentication Protocol).

³³ CHAP (Challenge-Handshake Authentication Protocol).

³⁴ WEB SITE: es el lugar en Internet donde todos, y en cualquier parte del mundo podrán visitarlo cuando quieran averiguar algo acerca de Ud.

- **Certificados Para WAP:** consienten a las Web comerciales existentes y de nueva creación la realización de transacciones seguras con los consumidores móviles.

Necesitan proporcionar seguridad y confianza a los usuarios potenciales, esta es la base para que se establezca una contraprestación que satisfaga a ambas partes.

Permiten mantener conexiones seguras basadas en encriptación y autenticación con dispositivos de telefonía móvil.

- **Certificados Personales:** otorgan seguridad a los correos electrónicos basados en un standard S/MIME. Podrá Firmar o cifrar los mensajes de correo para asegurarse de que sólo el receptor designado sea el lector de nuestro mensaje.
- **Ca's Corporativas:** es la solución óptima para las empresas que quieran disponer de un sistema de generación de cualquier tipo de Certificado para sus usuarios (trabajadores, proveedores, clientes, etc.) y servidores.

Una CA Corporativa puede generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código. En función del tipo de funcionalidad que se le quiera dar a la CA se deberá escogerse un diferente tipo de CA Corporativa.

- **Certificados Para Firmar Código:** permitirá a un administrador, desarrollador o empresa de software firmar su software (ActiveX, Applets Java, Plug-ins, etc.) y Macros, y distribuirlo de una forma segura entre sus clientes.
- **Certificados Para IPSEC-VPN:** son los elementos necesarios para que la empresa aproveche las cualidades y ventajas de la utilización de las VPNs³⁵ de un modo plenamente seguro. Las VPNs surgen como consecuencia de la creciente demanda de Seguridad en las comunicaciones ya sea entre Router-Router o Cliente-Servidor. La apertura de las redes corporativas a empleados remotos (con gran importancia en el caso del Teletrabajo), sucursales, business partners o clientes.

2.4.1.2 Control De Acceso (Autorización).

³⁵ VPNs Red Privada Virtual (RPV) aparece frecuentemente asociado a los de conectividad, [Internet](#) y seguridad.

Este servicio verifica que los recursos son utilizados sólo por quien tiene derecho a hacerlo. La forma más habitual de establecer autorizaciones es mediante ACL (Access Control Lists)³⁶.

2.4.1.3 Confidencialidad De Los Datos.

Con este servicio se evita que se revelen, deliberada o accidentalmente, los datos de una comunicación. El proceso empleado se llama encriptación donde se usan dos tipos de claves:

- **Criptografía De Clave Pública O Asimétrica:** confía dos tipos de claves para encriptar y desencriptar los datos. Esta clave es distribuida libremente entre los clientes.
- **Criptografía De Clave Privada O Simétrica:** utiliza la misma clave para encriptar y desencriptar los datos, por lo que es necesario que ambas partes conozcan dicha clave. Para intercambiar esta clave secreta común de un modo seguro se usa la encriptación asimétrica.

2.4.1.4 Integridad De Los Datos.

Este servicio verifica que los datos de una comunicación no se alteren, esto es, que los datos recibidos por el receptor coincidan por los enviados por el emisor. Las técnicas más habituales de comprobación de la integridad de un mensaje utilizan algoritmos de dispersión (hashed³⁷) sobre dicho mensaje que detectan el más leve cambio de contenido.

2.4.1.5 No Repudio.

³⁶ ACL (Access Control Lists).

³⁷ Hashed: contraseñas Hashed se cifran utilizando un algoritmo hash con valor salt unidireccional cuando se almacenan en la base de datos.

Proporciona la prueba, ante una tercera parte, de que cada una de las entidades ha participado en la comunicación. Puede ser de dos tipos:

- **Con Prueba De Origen O Emisor:** el destinatario tiene garantía de quien es el emisor concreto de los datos.
- **Con Prueba De Entrega O Receptor:** el emisor tiene prueba de que los datos de la comunicación han llegado íntegramente al destinatario correcto en un instante dado.

Por tanto, al hablar de seguridad, debemos especificar cuáles son los servicios de seguridad que requiere nuestro sistema y cómo vamos a garantizarlos.

2.4.1.6 Clonación Y Virus.

- La clonación consiste en copiar un teléfono celular para que las llamadas puedan ser realizadas desde la cuenta de un cliente sin su consentimiento. Debido a que no requiere que el teléfono sea físicamente robado, un usuario no sabrá que su teléfono ha sido clonado hasta que reciba la factura.

Un teléfono GSM³⁸ podría, en teoría, ser clonado, pero sólo abriéndolo y copiando la tarjeta SIM3. Este es un proceso difícil, que en términos estrictamente financieros, supone un coste mayor que las ganancias potenciales.

- Los virus son una amenaza para cualquier plataforma informática. No es probable que ataquen a los actuales teléfonos celulares, pero sólo porque su funcionalidad es limitada.

Con la llegada de la tercera generación, será posible conectarse directamente desde el ordenador de bolsillo y descargar y transmitir datos. Esto significa que será más fácil que se transmitan los virus. Los ordenadores de bolsillo tienen una capacidad limitada por lo que no pueden tener programas antivirus, ya que requieren gran cantidad de memoria.

2.5 LA SEGURIDAD EN WAP.

³⁸ GSM: es un servicio ofrecido por las empresas operadoras de [telefonía móvil](#) que permite determinar, con una cierta precisión, donde se encuentra físicamente un terminal móvil determinado.

En las conexiones a Internet desde dispositivos móviles, los datos son transferidos a través de diferentes canales: por aire, por la línea telefónica y sobre redes IP.

La seguridad que ofrecen los protocolos de telefonía móvil no es suficiente ya que están limitados a la etapa aérea.

Además, la fortaleza de los algoritmos criptográficos utilizados es altamente cuestionada ya que se ha comprobado que pueden ser rotos en pocos segundos por simples PCs.

2.5.1 Protocolo Inalámbrico De Seguridad A Nivel De Transporte (WTLS).

Es un protocolo de transporte seguro basado en el protocolo de seguridad en Internet TLS³⁹.

El WTLS incorpora el soporte a datagrama, un modo optimizado de intercambio de claves, y refresco dinámico de la clave de sesión para dificultar más los ataques en un medio de transmisión tan vulnerable a espías.

Admite la utilización de algoritmos criptográficos basados en curvas elípticas para el intercambio de claves que ofrecen algunas ventajas en cuanto a memoria y prestaciones.

El protocolo WTLS ofrece seguridad extremo-extremo entre los puntos finales del protocolo WAP.

Cuando la pasarela hace peticiones al servidor origen utiliza SSL bajo HTTP para obtener confidencialidad. Como los protocolos WTLS y SSL no son compatibles, los datos tienen que ser descifrados y vueltos a cifrar en la pasarela.

2.5.2 Librería Criptográfica Del Lenguaje Wmlscript Crypto Library (WMLS).

Las aplicaciones como el comercio electrónico requieren la capacidad de poder proporcionar pruebas persistentes de la autorización que alguien ha dado para hacer una determinada transacción.

WTLS proporciona autenticación transitoria del cliente para la duración de la conexión WTLS.

³⁹ TLS: Transport Layer Security (TLS) -Seguridad de la Capa de Transporte-, su sucesor, son [protocolos criptográficos](#) que proporcionan comunicaciones [seguras](#) en [Internet](#).

El navegador WAP incluye una función en la librería criptográfica de WMLScript, que asigna un campo de texto de un formulario WML. Una llamada a esta función permite asignar cualquier cadena de la página WML, que se mostrará por pantalla para pedir al usuario su confirmación.

Después que los datos hayan sido firmados y tanto la asignatura como los datos hayan sido enviados a través de la red, el servidor puede extraer la firma digital, validarla y guardarla para propósitos contables.

2.5.3 Módulo De Identidad Inalámbrico (WIM).

La funcionalidad de seguridad en WAP incluye el protocolo WTLS a nivel de transporte, y el WMLScript a nivel de aplicación.

Para dar seguridad óptima, las partes necesitan ser computadas en un dispositivo hardware protegido, de manera que un atacante no pueda extraer datos susceptibles. Estas funciones son las que incluyen datos sensibles, concretamente las claves privadas permanentes utilizadas en el establecimiento de conexión WTLS con autenticación de cliente y las claves que se utilizan en la generación de firmas electrónicas en el nivel de aplicación.

El módulo de Identidad WAP sirve para realizar la funciones de seguridad en WTLS y WMLScript, y especialmente, para guardar y procesar la información necesaria para identificar y autenticar al usuario.

2.6 ARQUITECTURA DE SEGURIDAD WAP.

Existen tres partes en el modelo de seguridad de WAP según se muestra en la figura 2.2

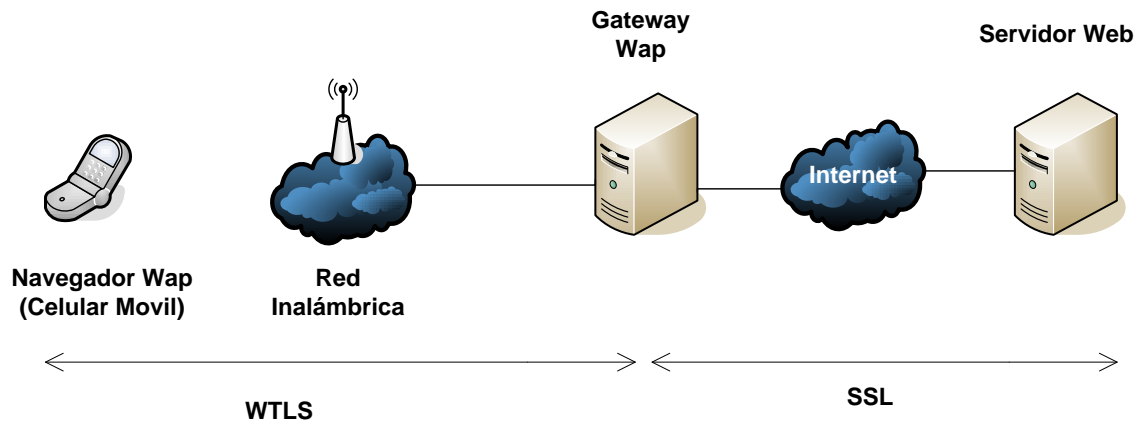


Figura 2.2: Modelo de Seguridad WAP⁴⁰.

- El Gateway WAP utiliza SSL para comunicarse de manera segura con un servidor Web, asegurando privacidad, integridad y autenticidad del servidor.
- El Gateway WAP utiliza WTLS para comunicarse de manera segura con el teléfono celular.
- El Gateway WAP proporciona un puente entre los protocolos de seguridad WTLS y SSL.

2.6.1 Zona Internet: El Puente Hacia El Servidor De Aplicaciones.

Utiliza el protocolo SSL (Secure Sockets Layer), que dispone un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él, como garante de la seguridad en el acceso a servicios "delicados", como compra (comercio electrónico) o transacciones bancarias entre otras.

El modo de funcionamiento de SSL se compone de dos partes diferenciadas.

- **Handshake Protocol (Apretón De Manos):** se encarga de establecer la conexión, verificando la identidad de las partes (opcionalmente) y determinando los parámetros que se van a utilizar posteriormente.
- **Record Protocol:** comprime, cifra, descifra y verifica la información que se transmite tras el inicio de la conexión (handshake⁴¹).

⁴⁰ Figura 2.2: Modelo de Seguridad WAP por <http://www.munisurquillo.gob.pe/website/libros/Inform%E1tica/Kewapo/Seguridad.pdf>.

El SSL, como protocolo de seguridad de transporte, sólo proporciona algunos de los servicios de seguridad necesarios:

- **Confidencialidad:** la información que circula entre el cliente (habitualmente un navegador) y el servidor, que actúa de frontal del servicio, se cifra utilizando criptografía de clave simétrica (con una clave de sesión acordada en el handshake).
- **Autenticación:** las partes que mantienen la comunicación se autentican mediante certificados basados en criptografía de clave pública. Esto no es siempre así, siendo lo más habitual que sea únicamente el servidor el que se autentica mediante un certificado digital.
- **Integridad:** la integridad de los datos transmitidos se asegura usando códigos de integridad (MAC) calculados mediante funciones de hash (SHA o MD5).

2.6.2 Zona Inalámbrica: Del Dispositivo WAP A La Pasarela.

Los dispositivos inalámbricos en esta zona se debe tener en cuenta varios aspectos tales como:

2.6.2.1 El Medio Aéreo (GSM).

El entorno GSM (Global System for Mobile Communications).

Los mecanismos de cifrado de GSM no son suficientes para garantizar la seguridad de cualquier transacción conducida mediante WAP, debido tanto a la debilidad de los algoritmos como a la porción de camino protegida, que sólo va desde el terminal móvil a la BTS (Estación transceptora base), como puede observarse en la figura 2.3.

Es una tecnología digital de acceso aéreo que incluye mecanismos de cifrado de la comunicación entre el terminal móvil y la BSC (estación base).

⁴¹ Handshake: Es el protocolo de comienzo de comunicación entre dos máquinas o sistemas.

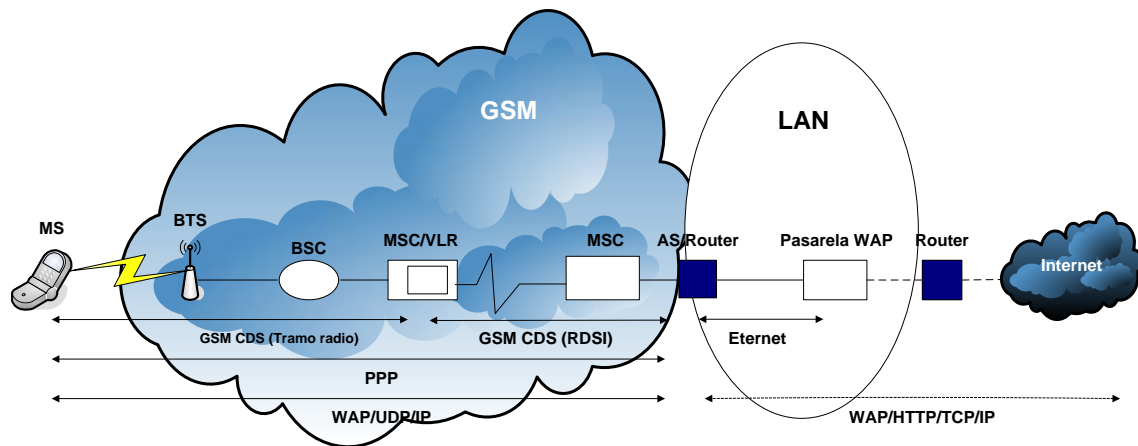


Figura 2.3: Arquitectura De Comunicaciones WAP⁴².

2.6.2.2 Wireless Transport Layer Security (WTLS).

La intención de los autores de WTLS fue tomar TLS y añadir soporte a datagramas, optimizar el tamaño de los paquetes transmitidos y seleccionar algoritmos rápidos entre los permitidos.

WAP ha definido WTLS siguiendo una serie de criterios:

- Debe soportar datagramas.
- Debe soportar portadoras de ancho de banda variopinto.
- Debe soportar retardos potencialmente largos.

La capacidad de memoria y procesamiento de los terminales puede ser pequeña.

Si se utiliza WTLS para el envío de mensajes seguros ofrece los siguientes servicios

- **Integridad de los datos:** se asegura que los datos intercambiados entre el terminal y la pasarela WAP no han sido modificados

⁴² Figura 2.3: Arquitectura De Comunicaciones WAP por <http://www.munisurquillo.gob.pe/website/libros/Inform%Edtica/Kewapo/Seguridad.pdf>.

- **Confidencialidad de los datos:** se asegura que la información intercambiada entre el terminal y la pasarela WAP no puede ser entendida por terceras partes que puedan interceptar el flujo de datos.
- **Autenticación:** el protocolo contiene servicios para autenticar el terminal y la pasarela WAP.
- **Protección por denegación de servicio:** asegura que las capas superiores del protocolo WAP están protegidas contra ataques por denegación de servicios (DoS, Denial of Service) mediante la identificación y reenvío de los mensajes no comprobados.
Existen tres tipos diferentes de seguridad, cada uno de ellos con sus requerimientos y características.
 - **Clase 1:** clase básica en la que no existe autenticación ni de cliente (terminal WAP) ni de pasarela WAP.
 - **Clase 2:** lo mismo que la clase 1, pero añadiendo autenticación de la pasarela WAP (este nivel es el equivalente al implementado usualmente con SSL en Internet).
 - **Clase 3:** igual que la clase 2, pero añadiendo autenticación de terminal WAP. En la actualidad no existe ningún terminal WAP que soporte la clase 3.

Características	Clase 1	Clase 2	Clase 3
Intercambio de clave pública	B	B	B
Certificado de servidor	O	B	B
Certificado de cliente	O	O	B
Establecimiento de clave secreta compartida	O	O	O
Compresión	-	O	O
Encriptación	B	B	B
MAC	B	B	B
Interfaz con tarjetas inteligentes	-	O	O

O = Opcional

B = Obligatorio

Tabla 2.1: Clases De La Implementación De Seguridad WTLS⁴³.

2.6.3 Zona Gris: La Pasarela WAP.

La pasarela WAP es la responsable de la transformación de los mensajes entre un protocolo a otro.

La pasarela debe desencriptar los mensajes codificados en formato TLS, convertirlos a binario, encriptarlos mediante WTLS y enviarlos. Esta operación se efectúa en el dispositivo WAP que recibe el mensaje.

Este proceso conlleva la posibilidad de que alguien consulte los mensajes en la pasarela de una forma totalmente legible (“white spot”). Sin embargo, existen barreras para dificultar esta posible violación de la privacidad.

- Las premisas de las pasarelas de un operador de red suelen estar localizadas en un centro de datos de alta seguridad.
- La transformación de los mensajes, incluyendo la encriptación, desencriptación y codificación, sucede en la memoria, sin la participación de ningún archivo temporal o una escritura explícita en el disco.
- Ningún detalle de esta operación es almacenado en los archivos históricos.
- El problema de la autenticación de usuario:

La ausencia de cifrado extremo a extremo no es la única debilidad del modelo WAP, se pierde también la autenticación de las partes (en SSL siempre se garantizaba, al menos, la del servidor).

En principio, la autenticación de los usuarios debe hacerse de modo similar como se hace con Internet, el modo más obvio es la utilización de un par identificador/clave integrado o no con la propia autenticación del servidor Web. Sólo es fiable si se utiliza un canal seguro (es decir, si se utiliza WTLS).

⁴³ Tabla1.1: Clases De La Implementación De Seguridad WTLS por <http://www.munisurquillo.gob.pe/website/libros/Inform%Edtica/Kewapo/Seguridad.pdf>.

2.6.4 Seguridad Extremo A Extremo.

WAP ofrece una arquitectura flexible de seguridad, centrándose en proporcionar un servicio con seguridad entre la conexión del usuario y un servidor WAP, es decir, en general no ofrece mecanismos de seguridad extremo a extremo entre el usuario del terminal móvil y el servidor Web de Internet.

Tipos de seguridad extremo a extremo:

(a) Confiar en el servidor WAP y utilizar el mecanismo de autenticación de la red móvil: en este caso se cede toda la autenticación del cliente a la propia red móvil, y el servidor WAP establece una conexión SSL con el servidor Web. Esta solución requiere confianza total en el servidor WAP, pero es fácilmente implantarle y en la red móvil no es necesario utilizar el protocolo WTLS.

(b) Confiar en el servidor WAP y utilizar WTLS entre cliente y servidor WAP: se aumenta la seguridad en la red móvil, pero nuevamente es necesaria una confianza total en el servidor. Requiere que los terminales móviles y el servidor WAP implementen WTLS.

(c) Utilizar una conexión WTLS con el servidor Web remoto: esta solución no requiere confianza en el servidor WAP (las medidas de seguridad se implementan extremo a extremo). A cambio, requiere que el servidor de Internet ofrezca un servidor WTLS.

(d) Proteger la comunicación a nivel de aplicación: ciertas aplicaciones críticas requerirán servicios especiales de seguridad (como no repudio) que forzosamente se deben ofrecer a nivel de aplicación.

En este caso el desarrollador es el principal responsable de configurar su infraestructura para administrar a los usuarios móviles que accederán a la aplicación.

Hoy en día, ésta es la única forma de garantizar comunicaciones extremo a extremo seguras entre un dispositivo WAP y un servidor de aplicaciones

CAPITULO III

ANÁLISIS DEL MÓDULO DEL SISTEMA ADMINISTRATIVO INTEGRADO FENIX.

3.1 SISTEMA ADMINISTRATIVO INTEGRADO FENIX.

Fénix es una herramienta enfocada a brindar solución inmediata a los problemas de procesamiento y obtención de resultados del área Contable, Financiera y Tributaria, vital para las empresas (PYMES⁴⁴).

Se encarga en optimizar las tareas diarias, aprovechar el tiempo, alcanzar un mayor rendimiento profesional, generar nuevos ingresos y acceder a potenciales clientes.

⁴⁴ PYMES: es el [acrónimo](#) de pequeñas y medianas empresas.

3.2 ALCANCE DEL SISTEMA.



Figura 3.1: Módulos del Sistema Administrativo Integrado FENIX.

- **Facturación:** es un documento que detalla los bienes o servicios vendidos o prestados por una parte a la otra, con indicación de cantidades y precios.
- **Punto De Venta (Pos):** es el proceso personal o impersonal por el que el vendedor comprueba, activa y satisface las necesidades del comprador para el mutuo y continuo beneficio de ambos (del vendedor y el comprador).
- **Compras:** implica vender bien las mercancías que tus clientes necesitan, también implica recuperar el costo de la compra y obtener una ganancia para la empresa.
- **Cientes – Cuentas X Cobrar:** son provenientes de Ventas de bienes o servicios. Este grupo de cuentas por cobrar está formado por aquellas cuyo origen es la venta a crédito de bienes o servicios y que, generalmente están respaldadas por la aceptación de una "factura" por parte del cliente.

- **Proveedores – Cuentas Por Pagar:** es la cuenta que corresponde únicamente a las deudas contraídas con los proveedores, respaldadas por sus facturas, se consideran pasivos por ser [obligaciones](#) que deben pagarse dentro del ciclo de operaciones.
- **Inventarios:** es el conjunto de mercancías o artículos que tiene la empresa para comerciar con aquellos, permitiendo la compra y [venta](#) o la fabricación primero antes de venderlos, en un periodo económico determinados.
- **Caja:** es maximizar los flujos disponibles para inversión y consumo.
- **Bancos:** son recursos generados por una empresa por medio de concesiones de créditos, inversiones en títulos e ingresos financieros percibidos en concepto de gastos cargados por aplazamiento de cobro a clientes.
- **Contabilidad:** es el conjunto coordinado de procedimientos y técnicas que proporcionan datos validos, luego de ordenar, clasificar, resumir y registrar hechos y operaciones económicas, que brinda información sobre la composición del patrimonio del ente.

3.3 INFORMES.

Fénix cuenta con un completo módulo de reportes el cual puede seguir creciendo de acuerdo a las necesidades de los clientes, cada uno de estos reportes puede ser modificado en su forma según la conveniencia del usuario.

Detalle De Informes:

- **Artículos.**
 - Listado de Artículos.
 - Resumen de Ventas de Artículos.
 - Movimientos de Inventarios.
 - Existencias de Artículos.
 - Resumen de Ventas por Grupos.
 - Índices de Consumo.
 - Resumen de Cálculo de Plano.
 - Etiquetas Adhesivas.

- Existencias de Artículos en Bodegas.
- Reporte Horizontal – Categoría Especial.
- Kardex de Artículos.
- Lista de Artículos sin Movimientos.
- Lista de precios Agrupados.
- Resumen de pedido de Artículos.
- Best Sellers.

- **Ventas.**
 - Resumen de Ventas (Forma de Pago).
 - Resumen de Facturación (IVA, Retenciones, Descuentos).
 - Resumen de Ventas por pedidos (Forma de Pago).
 - Resumen de Facturación por pedidos IVA, Retenciones, Descuentos).

- **Clientes.**
 - Estado de cuentas de clientes (CXC).
 - Resumen de saldos de cuentas por cobrar.
 - Listado de Clientes.
 - Comisión Vendedores.
 - Cartera Clientes.
 - Cobros Clientes.
 - Libro Diario Cuentas por Cobrar.
 - Venta detallada a clientes.
 - Lista de Descuentos a Clientes.
 - Comisión de cobranza con tipos de Precios.
 - Despacho a clientes desde salidas.
 - Lista de clientes sin movimientos.

- **Proveedores.**
 - Listado de Proveedores.
 - Estados de cuentas a Proveedores (CXP).
 - Resumen de saldos de cuentas por Pagar.
 - Resumen de Facturas de Compras (IVA).

- Compra Detallada a Proveedores.
- Cartera de Proveedores.
- Libro Diario Cuentas por Pagar.

- **Caja.**
 - Listados de Cuentas de Caja.
 - Movimientos de Caja.
 - Movimientos de Caja – Bancos (Depósitos).
 - Ingresos / Egresos de Caja.
 - Resumen de Caja.
 - Resumen de Saldos Diarios de Caja.

- **Bancos.**
 - Listado de Cuentas Bancarias.
 - Estado de Movimientos / Disponibilidad / Saldos.

- **Contabilidad.**
 - Plan de Cuentas.
 - Asientos Pendientes.
 - Libro Diario.
 - Libro Mayor.
 - Balance de Comprobación.
 - Estado de Resultados.
 - Balance General.
 - Análisis Financiero.

3.4 INFORMES ESTADÍSTICOS.

Fénix extiende el beneficio de sus informes presentándolos en forma de gráficos estadísticos en barras, pastel, columnas, etc., los cuales pueden ser creados o modificados por nuestros clientes de acuerdo su gusto y necesidad.

Detalle De Informes.

- **Artículos.**
 - Estadísticas de Artículos.
 - Artículos.
 - Grupos de Artículos.
 - Artículos / Periodo.
 - Grupos de Artículos / Periodo.
 - Estadísticas de Movimientos de Inventarios.
 - Artículos.
 - Grupos de Artículos.
 - Artículos / Periodo.
 - Grupos de Artículos / Periodo.

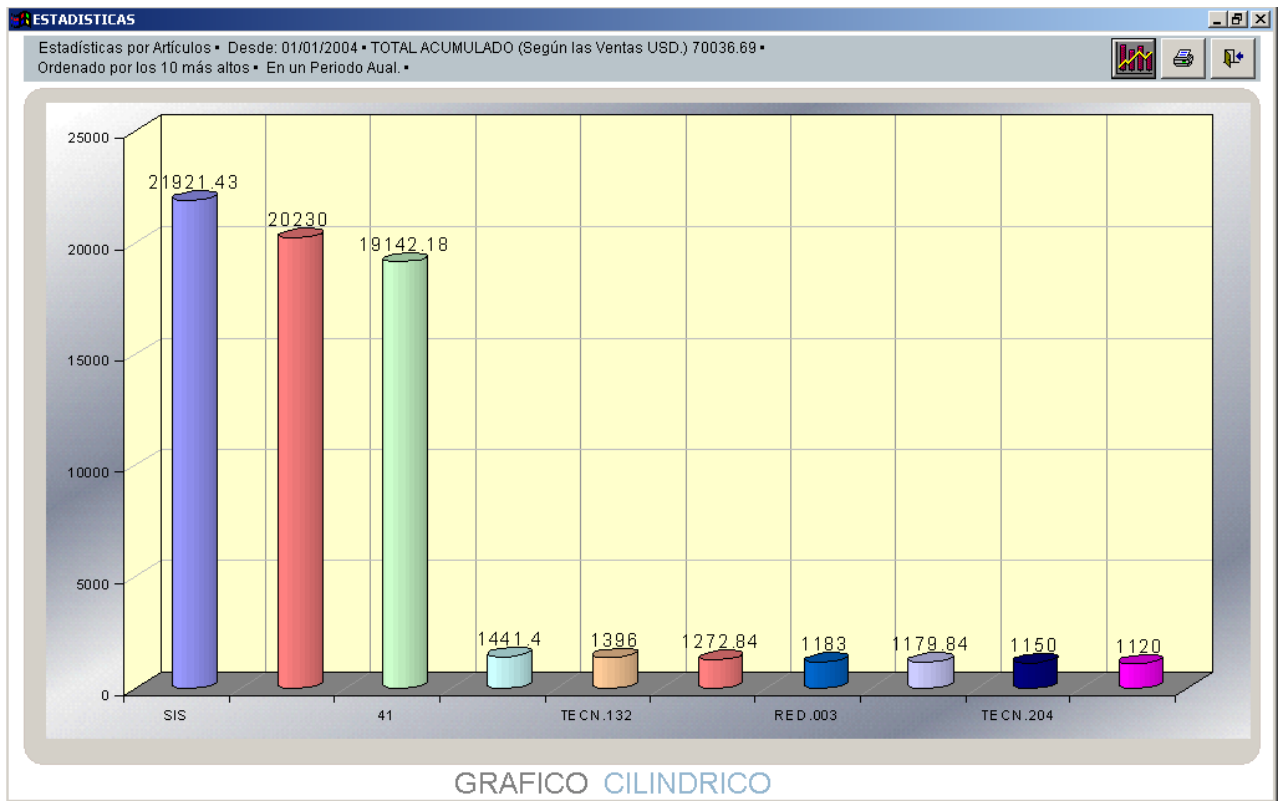


Figura 3.2: Gráfica De Estadísticas Por Artículo En Forma Cilíndrica.

- **Ventas.**

- Estadísticas de Ventas.
- Ventas por Clientes.
- Ventas Total de la empresa.

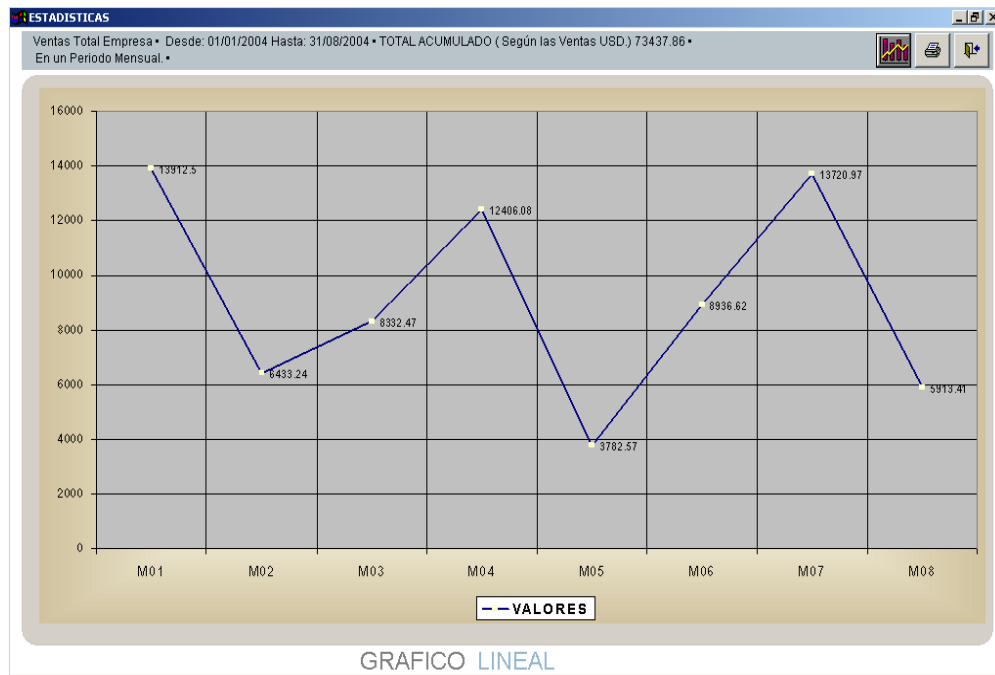


Figura 3.3: Gráfica De Estadísticas Por Ventas Total Empresa En Forma Lineal.

- Clientes.
- Estadísticas de Cartera de Clientes.

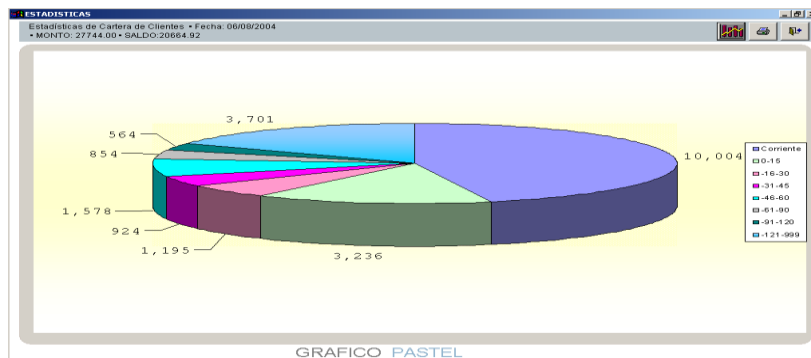


Figura 3.4: Gráfica De Estadísticas de Cartera de Clientes En Forma De Pastel.

- **Proveedores.**

- Estadísticas de Compras de Proveedores.
- Artículos.
- Grupos de Artículos.
- Artículos / Periodo.
- Grupos de Artículos / Periodo.
- Estadísticas Total de Compras.
- Compras a Proveedores.
- Compras Total Empresa.
- Estadística de Cartera de Proveedores.

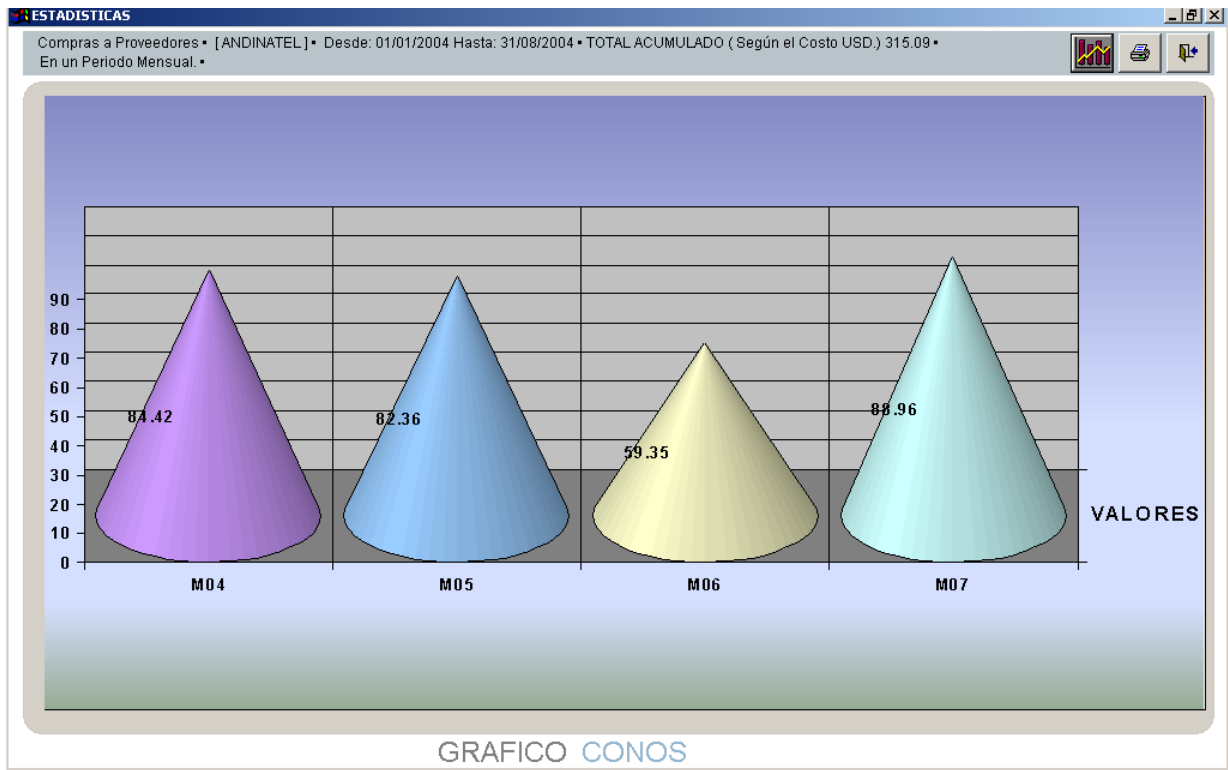


Figura 3.5: Gráfica De Estadísticas Compras a Proveedores En Forma De Conos.

- **Caja.**

- Estadísticas de Saldos en caja.

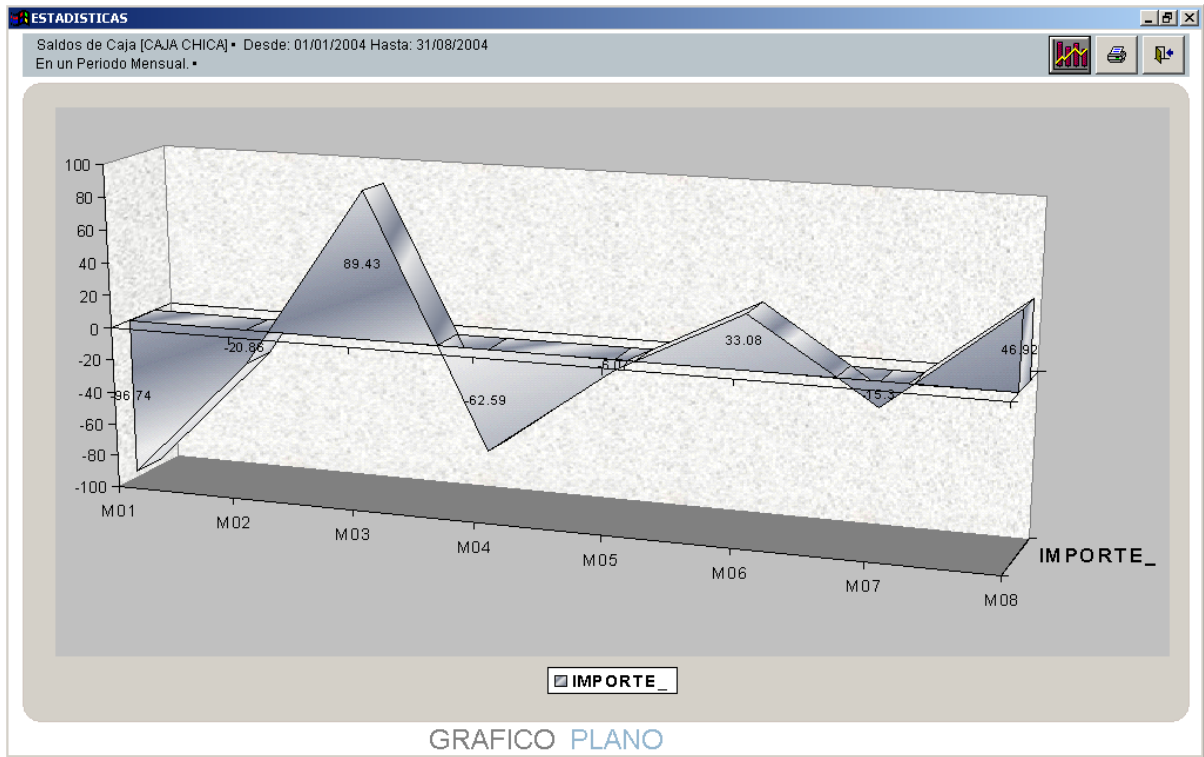


Figura 3.6: Gráfica De Estadísticas SalDOS De Caja En Forma de Plano.

- Bancos.
- Estadísticas de SalDOS Bancarios.

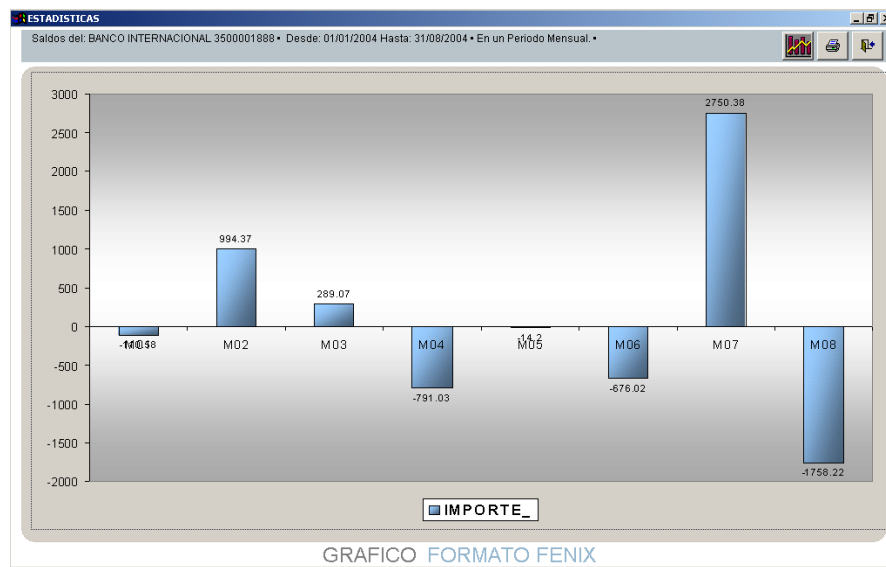


Figura 3.7: Gráfica De Estadísticas Por Saldos De Bancos En Formato FENIX.

3.5 CARACTERÍSTICAS.

- Interfase amigable y de fácil uso.
- Información en línea.
- Seguridad por niveles de acceso.
- Diseño estándar de Windows.
- Manejo rápido, óptimo e inteligente.
- Adaptable a las necesidades de su empresa.
- Reportes parametrizables.
- Ideal para trabajo en Red.
- Conexión Total con Microsoft Office.

3.6 VENTAJAS.

- Ilimitado Número de: líneas de productos, clientes, proveedores, vendedores, cajas, cuentas bancarias, empresas.
- Contabilización Automática.
- Comprobantes de Retención del IVA y retención en la fuente.
- Declaración del IVA y Retenciones en la fuente.
- Generación automática de informes para el SRI. (COA)
- Libre parametrización de porcentajes de impuestos (IVA, fuente).
- Conciliación Bancaria.
- Resumen de ventas por Vendedor.
- Cierres automáticos de caja y transferencia Caja – Bancos.
- Análisis de Cuentas por Cobrar y Pagar en línea.
- Análisis por Edades de Cuentas por Cobrar y Cuentas por Pagar.
- Creación Automática de Listas de Precios.
- Descuentos por Productos y/o Clientes.
- Cupo Máximo de Crédito por Cliente.
- Pagos Automáticos por Grupos de Facturas sobre un mismo cliente y proveedor.
- Inventario según Materia Prima, Prod. en Proceso, Prod. Terminado.
- Código de Barras.
- Inventario Periódico o Permanente.
- Rotación de Inventarios para la elaboración automática de Pedidos.

- Registro de pedidos de clientes y proformas.
- Facturación automática sobre pedidos y proformas.
- Facturación reversa.
- Resumen y Detalle del Estado de Cuentas de los Clientes.
- Relación Ventas por: Vendedor – Línea – Cliente.
- Informe Diario Ventas por Punto de Venta.
- Informe Diario del movimiento de ventas.
- Resumen Impuestos por Compras – Ventas.
- Rotación y cobertura de Inventarios.
- Saldos y Auxiliar de Caja – Bancos.
- Relación de Cartera por Vendedor.
- Kardex.
- Libre Parametrización de Reportes.
- Soporte Técnico Local.
- Solución inmediata con conexión remota, vía MODEM.
- Migración de Datos desde otros sistemas.

3.7 DESCRIPCIÓN DE LOS MÓDULOS.

3.7.1 Contabilidad General.

Agiliza el registro de asientos, la obtención de mayores, balances de saldos, integrados con alta consistencia y eliminación de errores.

Se integra con todos los módulos auxiliares (cuentas por cobrar, cuentas por pagar, facturación, compras, caja, bancos, etc.) combinando agilidad operativa con un ordenamiento lógico de la tarea y gran adaptabilidad a cada estilo de trabajo.

Obtiene en forma rápida y sencilla los estados contables finales a partir de la información generada en los diferentes auxiliares.

Este Sistema genera información de diversos aspectos requerida por le SRI para múltiples presentaciones impositivas.

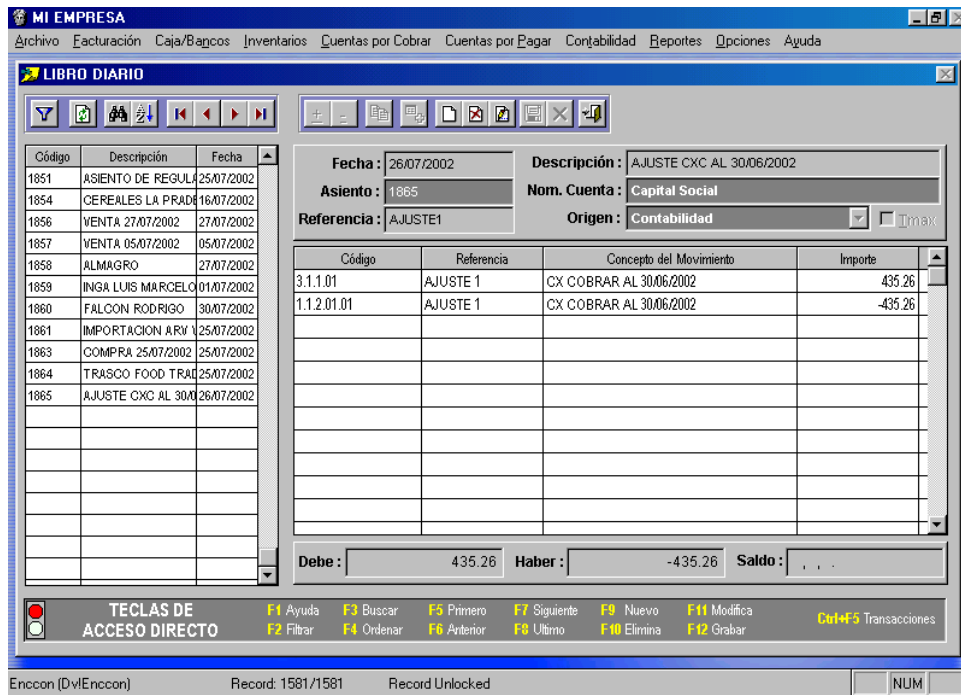


Figura 3.8: Gráfica Del Libro Diario.

La contabilización es realizada en base a definiciones contables especificadas por el contador, migrando la información que se requiera desde los módulos integrados, manteniendo una integridad total entre los mayores y los auxiliares.

3.7.2 Facturación.

Facturas / Devolución a Clientes

F000000382 Referencia: 012477

SANCHEZ LUCIA

Factura	Emisión	Total	Pag
012337	16/07/2002	\$420.00	<input type="checkbox"/>
012477	26/07/2002	\$748.00	<input type="checkbox"/>
0000013980	13/11/2002	\$461.00	<input type="checkbox"/>

Emitido en: 26/07/2002 Vence: 15/08/2002 Forma pago: CREDITO Tarifa: A Pagado

FACTURA # 012477

CANGUIL 50 LB / 16

Código	Artículo	Cantidad	Precio unit.	Desc.	%Iva	Total neto
CGL002	CANGUIL 50 LB	30.0000	11.20	0.00%	0.00%	\$336.00
AVE002	AVENA PRODICEREAL 25	40.0000	10.30	0.00%	0.00%	\$412.00

Subtotal	\$748.00	Flete	\$0.00	Efec.	\$ 0.00	Cam.	\$ 0.00
Descuento	0.00%	\$0.00	Ret. Fnt:	\$0.00	Total Fac:	\$748.00	
IVA	12.00%	\$0.00	Ret. IVA:	\$0.00	A Pagar :	\$ 748.00	

TECLAS DE ACCESO DIRECTO

F1 Ayuda	F3 Buscar	F5 F7	F9 Nuevo	F11 Modifica
F2	F4 Profomas	F6 F8	F10 Elimina	F12 Grabar

Figura 3.9: Gráfica De Factura/Devolución a Clientes.

Este módulo es totalmente funcional para ser acoplado a cualquier necesidad del usuario, permitiendo una facturación rápida y en línea, puede manejar varias opciones y puntos de venta, al mismo tiempo. Facilita la elaboración de facturas múltiples y automáticas en base a pedidos y proformas de clientes.

3.7.3 Inventarios.

Permite gestionar el control de existencias por almacén, piezas, modelos, tallas. Ofrece la posibilidad de realizar inventarios físicos y ajustarlos con el estadístico del sistema en forma automática. Controla los movimientos de artículos a través de una innovadora herramienta de selección múltiple de información por filtros, sin tener que emitir reportes.

Artículo	Fecha	Tipo	Documento	Cantidad	Costo u.	Precio u.	Origen
19	09/12/2002	EN	C000000156	10.00	\$50.00	\$0.00	CPA
19	09/12/2002	SA	F000000805	1.00	\$50.00	\$170.00	FAC
19	09/12/2002	SJ	I000000058	1.00	\$50.00	\$0.00	REC
19	09/12/2002	EJ	I000000059	1.00	\$50.00	\$0.00	REC

ANILLO DE RUBI			En Stock:	9.00	
Código	19	Cantidad	10.000	Costo unit.	\$50.0000
Fecha	09/12/2002	Documento	C000000156	Precio unit.	
Origen	COMPRA	Referencia		Costo total	\$500.0000
Tipo	+ ENTRADA COMPRAS				

TECLAS DE ACCESO DIRECTO	F1 Ayuda	F3 Filtar	F5 F6	F7 F8	F9 Nuevo	F11 Modifica
	F2	F4	F6	F8	F10 Elimina	F12 Grabar

Figura 3.10: Gráfica De Movimientos de Inventario.

3.7.4 Caja – Bancos.

Los movimientos son generados desde los módulos relacionados con caja y bancos en el manejo de cartera de clientes y proveedores, además permite registrar otros movimientos extras en estos auxiliares. Permite el manejo y control de cheques posfechados. La transferencia desde caja a bancos se la puede realizar en forma automática generando los depósitos y asientos contables, manteniendo un control documentando.

Doc. Origen	Fecha	Org	Tip	Pag	Importe	Caja	Doc. Pago
<input checked="" type="checkbox"/> F11826	01/07/02	CXC	CA	CH	1,271.40	01	R/C146
<input checked="" type="checkbox"/> F11878	01/07/02	CXC	CA	CH	147.00	01	R/C.146.2
<input checked="" type="checkbox"/> F11827	01/07/02	CXC	CA	CH	208.00	01	R/C.146.3
<input checked="" type="checkbox"/> F11286	02/07/02	CXC	CA	CH	2,504.70	01	R/C146.6
<input checked="" type="checkbox"/> F11755	02/07/02	CXC	AB	CH	33.68	01	R/C148.1
<input checked="" type="checkbox"/> F11678	02/07/02	CXC	CA	CH	526.84	01	R/C148.2
<input type="checkbox"/> F11688	02/07/02	CXC	CA	CH	105.00	01	R/C148.3
<input type="checkbox"/> F11703	02/07/02	CXC	CA	CH	287.20	01	R/C148.4

Banco	BANCO PICHINCHA CTA. CTE 009426537 00!	CH día:	\$134,655.86	\$ 4,691.62		
Fecha	30/06/2002	No.Doc.	001	CH Post:	\$ 0.00	\$ 0.00
Concepto	SALDO INICIAL	Efectivo:	\$ 73,488.05	\$ 0.00		
Beneficiario		Total:	\$ 0.00	\$ 4,691.62		

TECLAS DE ACCESO DIRECTO	F1 Ayuda	F3 Filtar	F5 F6	F7 F8	F9 Nuevo	F11 Modifica
	F2	F4	F6	F8	F10 Elimina	F12 Grabar

Figura 3.11: Gráfica De Depósitos.

3.7.5 Clientes – Proveedores.

Permite un ágil registro de cobranzas a clientes y pagos a proveedores con la posibilidad de indicar los comprobantes cancelados y los medios de pago utilizados.

Refleja a través de una amplia gama de informes los movimientos de las cuentas corrientes, la composición de saldos y la aplicación de comprobantes, entre otros aspectos.

Con esta herramienta, se podrá administrar las cuentas a cobrar y pagar visualizando los movimientos en línea y emitiendo informes de cuentas corrientes como la composición de saldos y resúmenes de cuentas.

Documento	Ultimo Pago	Saldo
F11822	30/06/2002	\$0.00
F000000061	04/07/2002	\$0.00
F000000388	26/07/2002	\$48.00
F000000786	14/11/2002	\$50.00
Total cobros pendientes:		\$98.00

Tipo	Emision	Importe	Origen
FC	30/06/2002	\$28.00	CXC
CA	03/07/2002	\$-28.00	CXC

Origen: CUENTA POR COBR | Emisión: 30/06/2002 | Vence: 30/06/2002 | Envío: 30/06/2002
Tipo: FACTURA | Concepto: SALDO INICIAL
Documento: F11822 | Importe: \$ 28.00 | Forma pago: [dropdown]
Referencia: [input] | No. pago: [input]
Pago Multiple: F | Asient Cont: [input]

TECLAS DE ACCESO DIRECTO: F1 Ayuda, F2, F3, F4, F5, F6, F7, F8, F9 Nuevo, F10 Elimina, F11 Modifica, F12 Grabar

Figura 3.12: Gráfica De Movimientos de Cuentas Por Cobrar A Clientes.

Permite al usuario realizar cancelaciones de varias facturas en cuentas por cobrar y pagar, con un solo documento de cobro o pago, reduciendo el tiempo de proceso al registrar varias transacciones individuales.

3.8 CON EL SISTEMA INTEGRADO FENIX.

Optimiza: su control de facturación mediante la creación de pedidos por cliente, y transacciones por vendedor con claves de acceso y permisos únicos.

Reduce: tiempos y procesos de contabilización, gracias al motor de definiciones contables que interactúa con el usuario para el registro de asientos en forma automática.

Extraiga: toda la potencia a los sistemas operativos Windows 9X, 2000, XP, así como a los nuevos microprocesadores, gracias a su arquitectura de 32 bits. Mayor rendimiento, mayor velocidad y óptima utilización de la memoria disponible en su computador.

Ajuste: el control de existencias, genere inventarios y realice un seguimiento total de movimientos que le permitan mantener inventarios sanos de muy buena rotación y rentabilidad.

Descubra: nuevas posibilidades de gestión para una toma de decisiones acertada, con una gama amplia de reportes en todos los módulos auxiliares.

CAPITULO I V

DESARROLLO DEL MÓDULO CARTERA DE CLIENTES (CUENTAS POR COBRAR) DEL SISTEMA ADMINISTRATIVO INTEGRADO FENIX A UN LENGUAJE WML CON PHP (APLICANDO LA METODOLOGÍA XP).

4.1 METODOLOGÍA.

Para la construcción del software se implementa la metodología XP (Programación Extrema), la cual comprende cuatro fases y/o etapas que se observan.

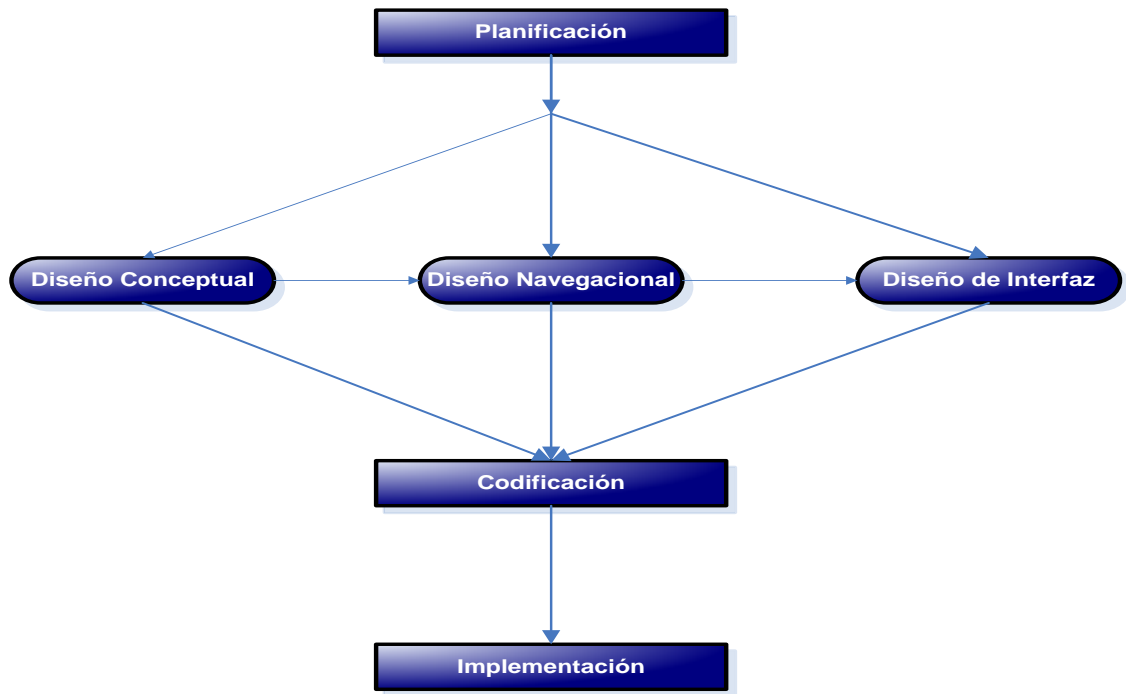


Figura 4.1: Fases De La Propuesta Metodológica XP.

4.2 PLANIFICACIÓN.

4.2.1 Especificación de Requisitos de Software.

4.2.1.1 Introducción.

Este documento contempla los requisitos necesarios y fundamentales para que el MODULO CARTERA DE CLIENTES (CUENTAS POR COBRAR) DEL SISTEMA ADMINISTRATIVO INTEGRADO FENIX orientado a tecnología WAP cumpla.

4.2.1.2 Requisitos Específicos.

Por la complejidad de la aplicación se han dividido en dos grupos los requisitos:

4.2.1.2.1 No Funcionales.

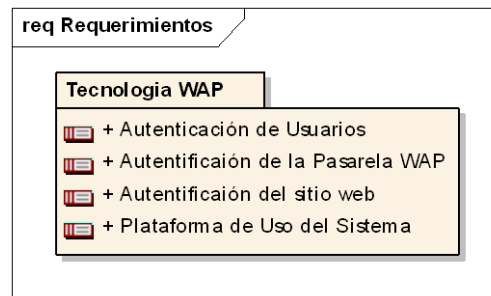


Figura 4.2: Requisitos no Funcionales.

Tecnología WAP.

El sistema debe cumplir con los requisitos correspondientes para su funcionamiento:

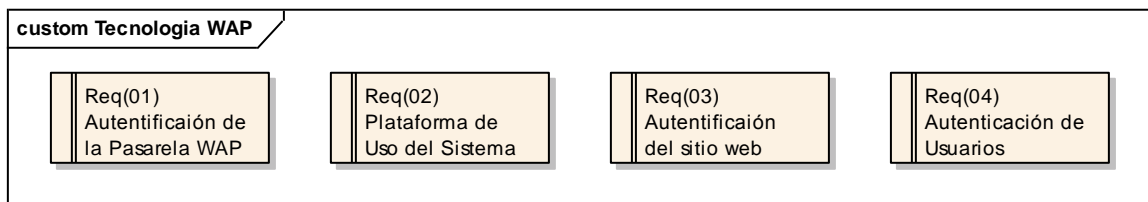


Figura 4.3: Requisitos para El Funcionamiento de la Aplicación.

Autenticación de Pasarela WAP.

Req(01) El sistema utilizara la capa de aplicación WTLS en la pasarela WAP para la comunicación segura.

Plataforma de Uso del Sistema.

Req(02) El sistema solo podrá ser usado por dispositivos móviles (teléfono celular) utilizando tecnología WAP.

Autenticación del Sitio Web.

Req(03) El sistema utilizara certificación usando un modulo SSL en el servidor Web para certificar el sitio Web.

Autenticación de Usuario.

Req(04) La aplicación utilizara el método md5 para la encriptación de password de clave de cada uno de usuarios a fin de salvaguardar la información del sistema.

4.2.1.2.2 Funcionales.

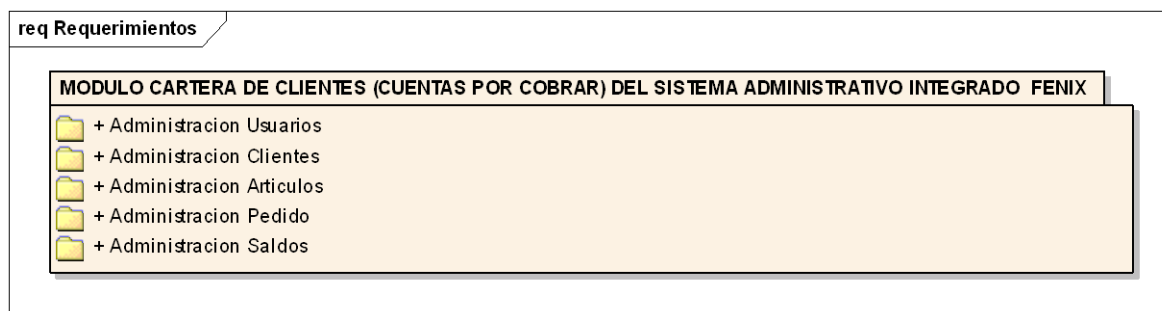


Figura 4.4: Requisitos Funcionales.

Modulo Cartera de Clientes (Cuentas por Cobrar) Del Sistema Administrativo FENIX.

El modulo debe estar conformado por:

Administración de Usuarios.

El sistema permitirá almacenar y mantener una lista de cuentas de usuarios en un repositorio persistente.

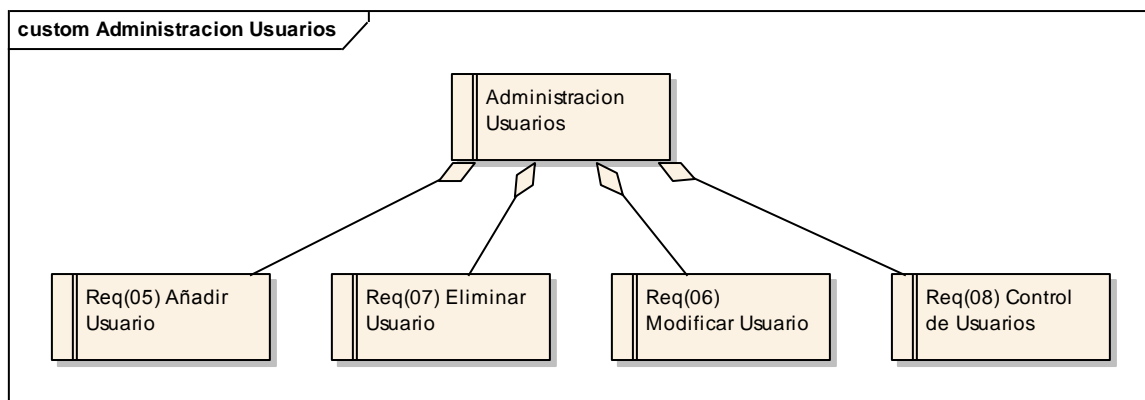


Figura 4.5: Requisitos Administración de Usuarios.

Añadir Usuarios.

Req(05) El sistema permitirá crear nuevos usuarios y ser almacenados en un repositorio persistente.

Modificar Usuarios.

Req(06) El sistema permitirá modificar usuarios existentes en un repositorio persistente.

Eliminar Usuarios.

Req(07) El sistema permitirá eliminar usuarios de un repositorio persistente.

Control de Usuarios.

Req(08) El sistema permitirá controlar el acceso de usuarios existentes en un repositorio persistente al sistema.

Administración de Clientes.

El sistema permitirá almacenar y mantener una lista de cuentas de clientes en un repositorio persistente.

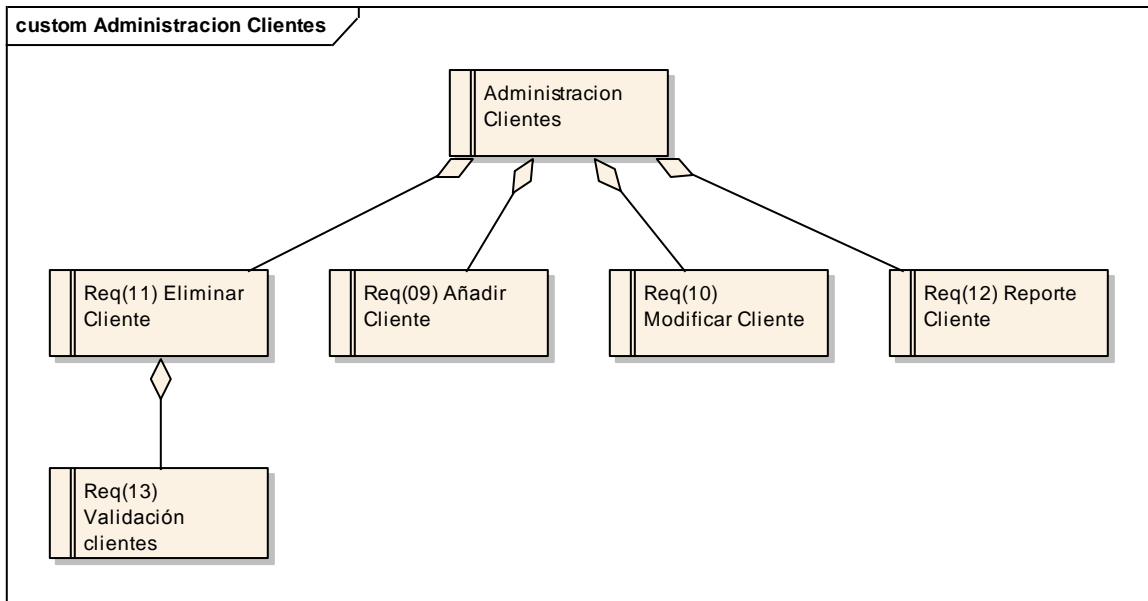


Figura 4.6: Requisitos Administración de Clientes.

Añadir Clientes.

Req(09) El sistema permitirá crear nuevos clientes y ser almacenados en un repositorio persistente.

Modificar Clientes.

Req(10) El sistema permitirá modificar clientes almacenados en un repositorio persistente.

Eliminar Clientes.

Req(11) El sistema permitirá eliminar clientes almacenados en un repositorio persistente.

Reporte de Clientes.

Req(12) El sistema permitirá mostrar clientes almacenados en un repositorio persistente.

Validación Clientes.

Req(13) El sistema permitirá eliminar clientes almacenados en un repositorio persistente siempre y cuando no estén registrados en pedidos pendientes.

Administración de Artículos.

El sistema permitirá almacenar y mantener una lista de cuentas de artículos en un repositorio persistente.

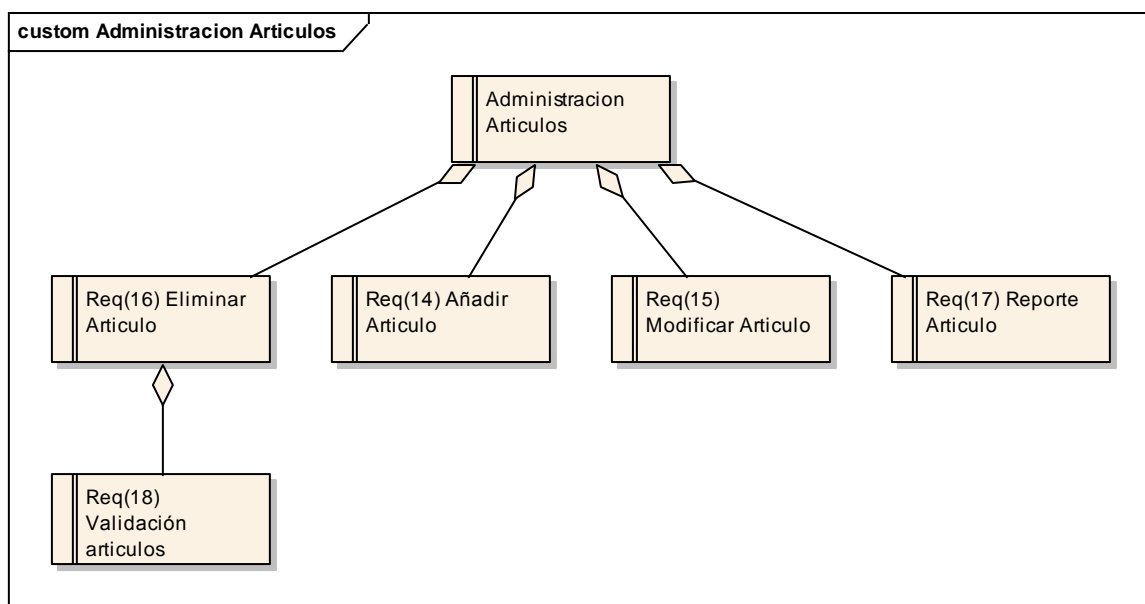


Figura 4.7: Requisitos Administración de Artículos.

Añadir Artículos.

Req(14) El sistema permitirá crear nuevos artículos y ser almacenados en un repositorio persistente.

Modificar Artículos.

Req(15) El sistema permitirá modificar artículos almacenados en un repositorio persistente.

Eliminar Artículos.

Req(16) El sistema permitirá eliminar artículos almacenados en un repositorio persistente.

Reporte de Artículos.

Req(17) El sistema permitirá mostrar artículos almacenados en un repositorio persistente.

Validación Artículos.

Req(18) El sistema permitirá eliminar artículos almacenados en un repositorio persistente siempre y cuando no estén registrados en pedidos pendientes.

Administración de Pedidos.

El sistema permitirá almacenar y mantener una lista de cuentas de pedidos en un repositorio persistente.

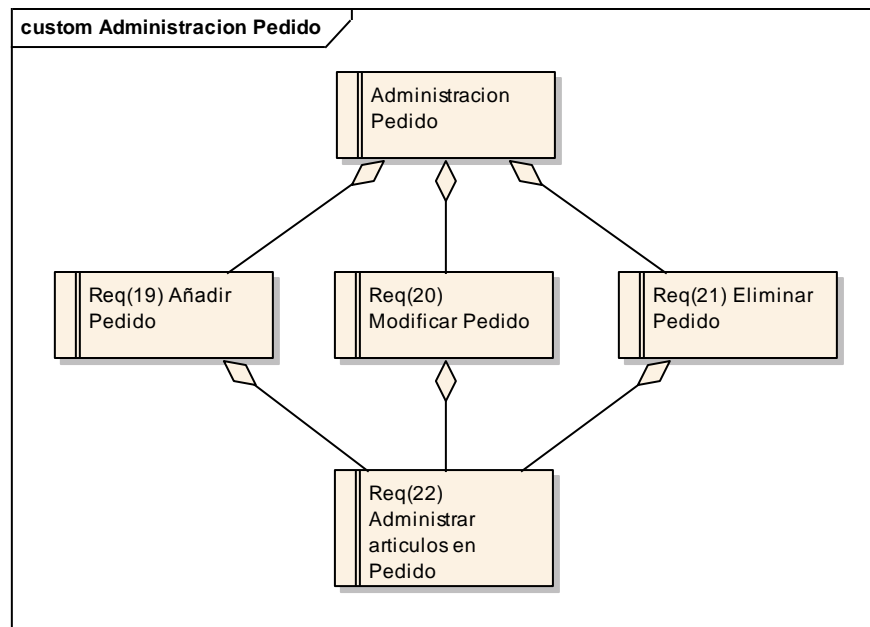


Figura 4.8: Requisitos Administración de Pedidos.

Añadir Pedidos.

Req(19) El sistema permitirá crear nuevos pedidos y ser almacenados en un repositorio persistente.

Modificar Pedidos.

Req(20) El sistema permitirá modificar pedidos almacenados en un repositorio persistente.

Eliminar Pedidos.

Req(21) El sistema permitirá eliminar pedidos almacenados en un repositorio persistente.

Administración de Artículos.

Req(22) El sistema permitirá administrar un artículo en un pedido y ser almacenados en un repositorio persistente.

Administración de Saldos.

El sistema permitirá almacenar y mantener una lista de cuentas de saldos en un repositorio persistente.

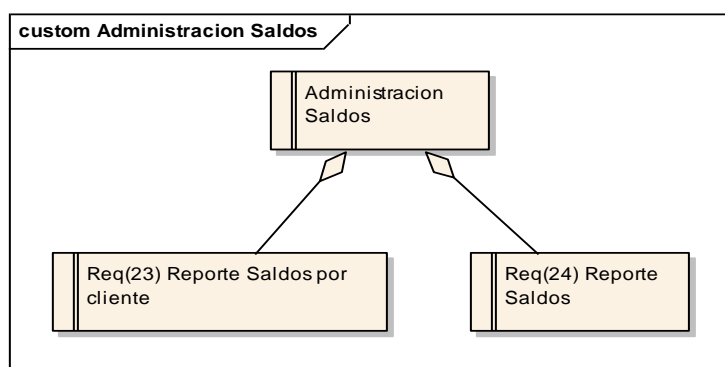


Figura 4.9: Requisitos Administración de Saldos.

Reporte de Saldos por Clientes.

Req(23) El sistema permitirá buscar saldos por cliente almacenados en un repositorio persistente.

Reporte Saldos.

Req(24) El sistema permitirá mostrar saldos almacenados en un repositorio persistente.

4.2.2 Usabilidad.

Tiempo Requerimiento de Entrenamiento.

Se requiere que el sistema sea fácil de comprender y manejar, estimado que el tiempo requerido de entrenamiento sea no mas de 1 Hora.

Interfaz de Administrador.

El sistema contara con una interfase de administración vía Web, se usara PHP para realizarla, y serán usadas por el usuario por medio de un servido Web Apache.

Interfaz de Usuario.

El sistema contara con una interfase de usuario vía WAP, se usara WML con PHP para realizarla, y serán usadas por el usuario por medio de un servido Web Apache teniendo comunicación con el servidor WAP para su interpretación en los dispositivos móviles (teléfono celular).

4.3 DISEÑO.

Se subdivide en tres etapas o fases:

4.3.1 Diseño Conceptual.

4.3.1.1 Casos de Uso.

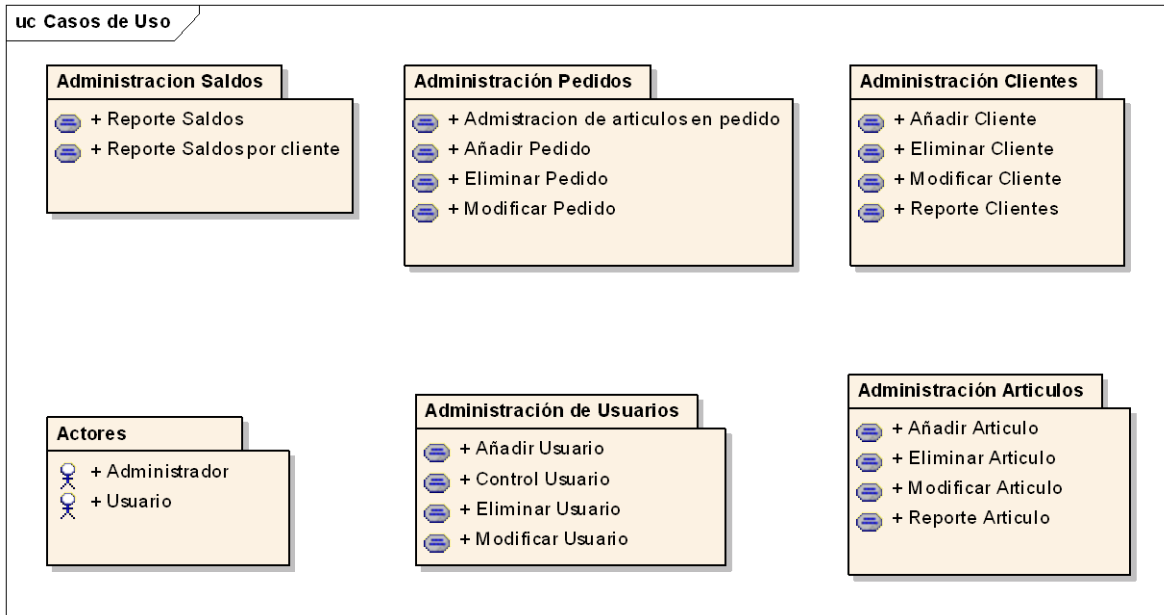


Figura 4.10: Casos de Uso.

Actores.

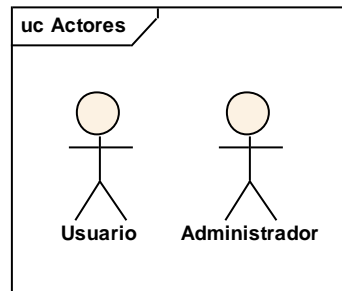


Figura 4.11: Actores.

Administrador.

El administrador del sistema es la persona encargada de manejar la administración de usuarios realizando sus acciones de manera correcta.

Usuario.

El usuario es la persona que utiliza el sistema y puede intervenir en la administración de clientes, artículos, pedidos y saldos realizando sus acciones de manera correcta.

Administración de Usuarios.

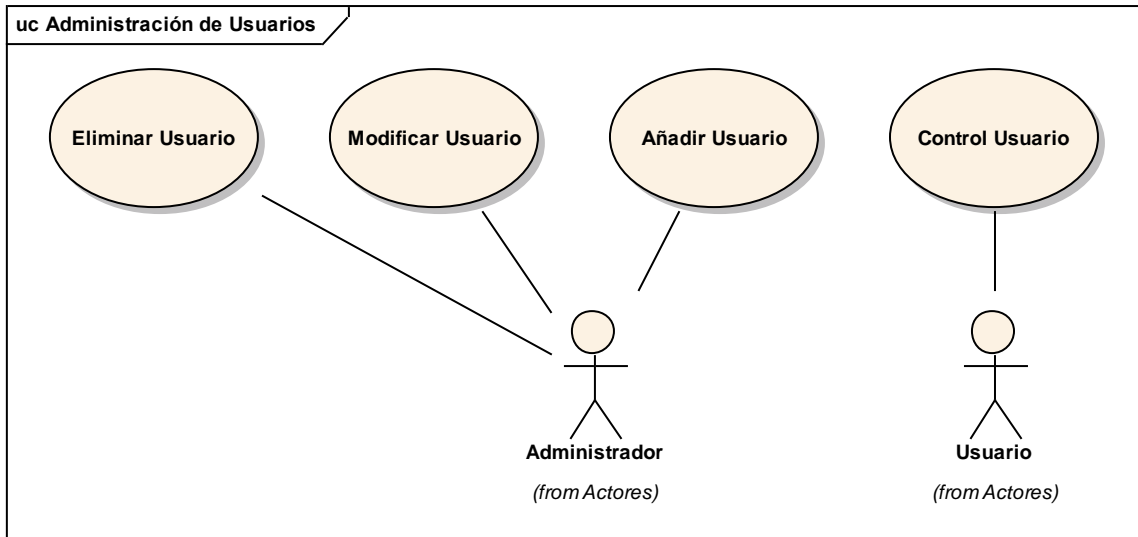


Figura 4.12: Casos de Uso Administración de Usuarios.

Nombre Caso de Uso: Añadir Usuario.

Actor: Administrador.

Tipo: Primario.

Descripción: El administrador añade los datos de un usuario termina caso de uso.

Nombre Caso de Uso: Modificar Usuario.

Actor: Administrador.

Tipo: Primario.

Descripción: El administrador modifica los datos de un usuario, verifica termina caso de uso.

Nombre Caso de Uso: Eliminar Usuario.

Actor: Administrador.

Tipo: Primario.

Descripción: El administrador elimina los datos de un usuario termina caso de uso.

Nombre Caso de Uso: Control de Usuario.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario ingresa al sistema los datos del usuario ya registrado termina caso de uso.

Administración de Clientes.

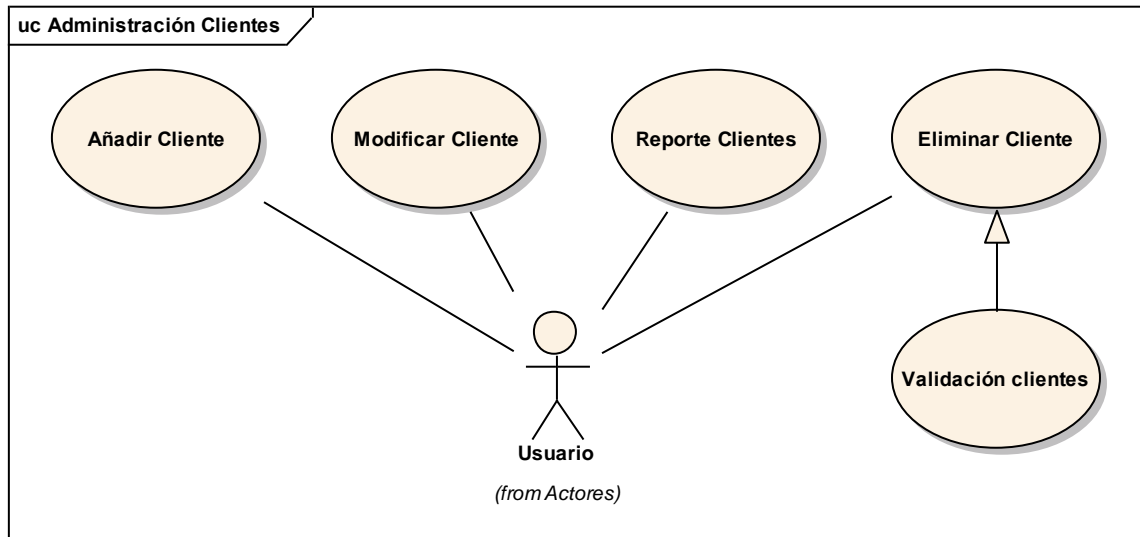


Figura 4.13: Casos de Uso Administración Clientes.

Nombre Caso de Uso: Añadir Cliente.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario añade los datos de un cliente termina caso de uso.

Nombre Caso de Uso: Modificar Cliente.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario modifica los datos de un cliente, verifica termina caso de uso.

Nombre Caso de Uso: Eliminar Cliente.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario elimina los datos de un cliente termina caso de uso.

Nombre Caso de Uso: Reporte Cliente.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario reporta todos los datos de los clientes registrados en el sistema termina caso de uso

Nombre Caso de Uso: Validación Cliente.

Actor: Usuario.

Tipo: Extendido.

Descripción: El usuario elimina los datos de un cliente si no esta relacionado con un pedido o saldos terminar caso de uso.

Administración Artículos.

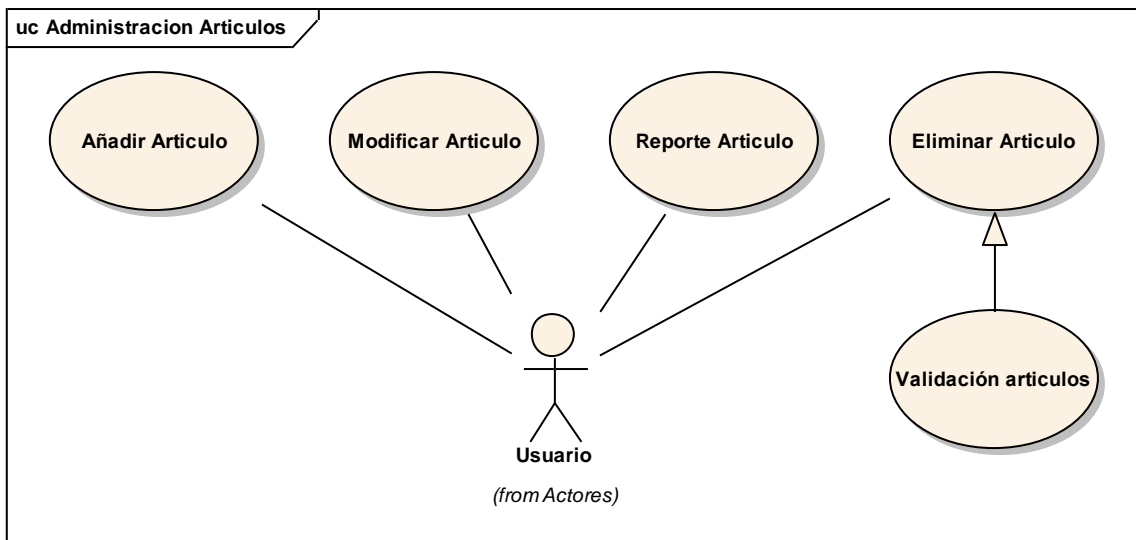


Figura 4.14: Casos de Uso Administración Artículos.

Nombre Caso de Uso: Añadir Artículo.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario añade los datos de un artículo termina caso de uso.

Nombre Caso de Uso: Modificar Artículo.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario modifica los datos de un artículo, verifica termina caso de uso.

Nombre Caso de Uso: Eliminar Artículo.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario elimina los datos de un artículo termina caso de uso.

Nombre Caso de Uso: Reporte Artículo.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario reporta todos los datos de los artículos registrados en el sistema termina caso de uso.

Nombre Caso de Uso: Validación Artículo.

Actor: Usuario.

Tipo: Extendido.

Descripción: El usuario elimina los datos de un artículo si no esta relacionado con un pedido terminar caso de uso.

Administración Artículos.

Administración de Pedidos.

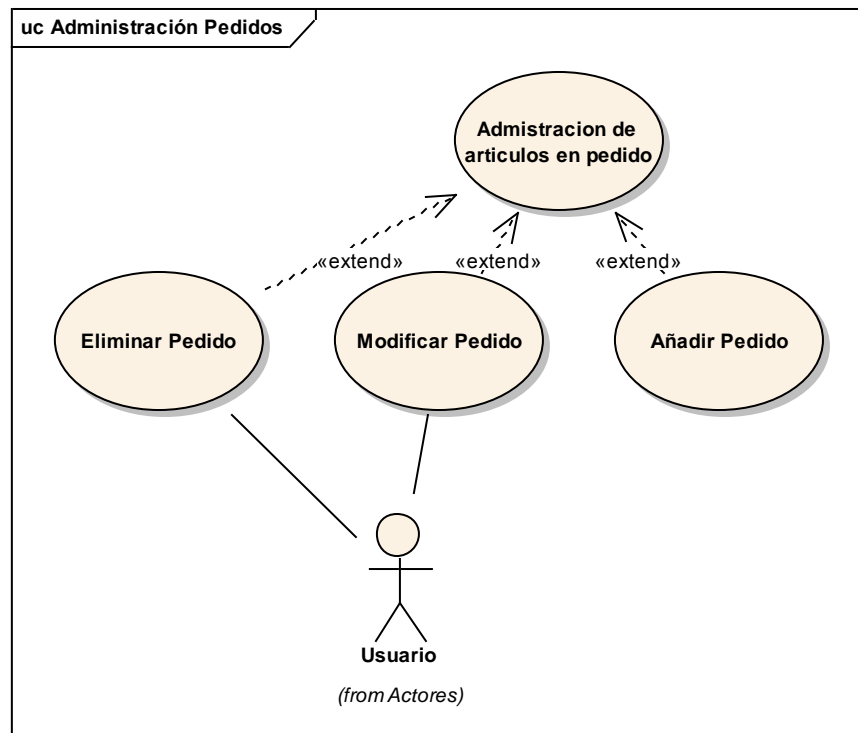


Figura 4.15: Caso de Uso Administración Pedidos.

Nombre Caso de Uso: Añadir Pedido.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario añade los datos de un pedido termina caso de uso.

Nombre Caso de Uso: Modificar Pedido.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario modifica los datos de un pedido, verifica termina caso de uso.

Nombre Caso de Uso: Eliminar Pedido.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario elimina los datos de un pedido termina caso de uso.

Nombre Caso de Uso: Administración de Artículos en Pedido.

Actor: Usuario.

Tipo: Extendido.

Descripción: El usuario añade, modifica, elimina los datos de un articulo en un pedido termina caso de uso.

Administración de Saldos.

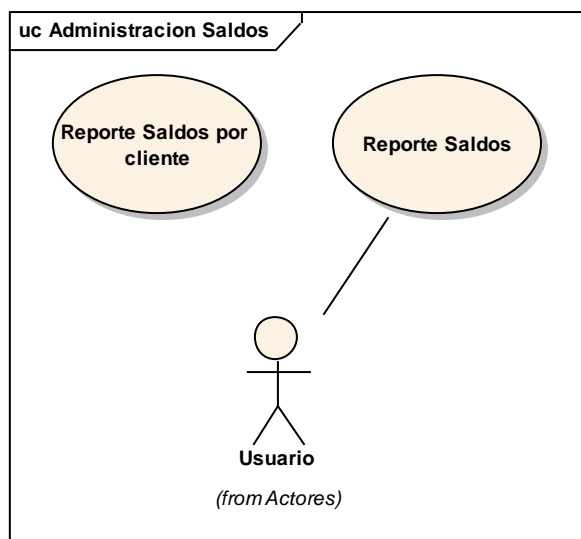


Figura 4.16: Casos de Uso Administración de Saldos.

Nombre Caso de Uso: Reporte Saldos por Cliente.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario reporta los datos de un saldo por un dato de un cliente registrado en el sistema termina caso de uso.

Nombre Caso de Uso: Reporte Saldos.

Actor: Usuario.

Tipo: Primario.

Descripción: El usuario reporta todos los datos del saldos registrados en el sistema termina caso de uso.

4.3.1.2 Diagrama de Secuencia.

Administración del Sistema.

Ingreso Al Sistema WAP.

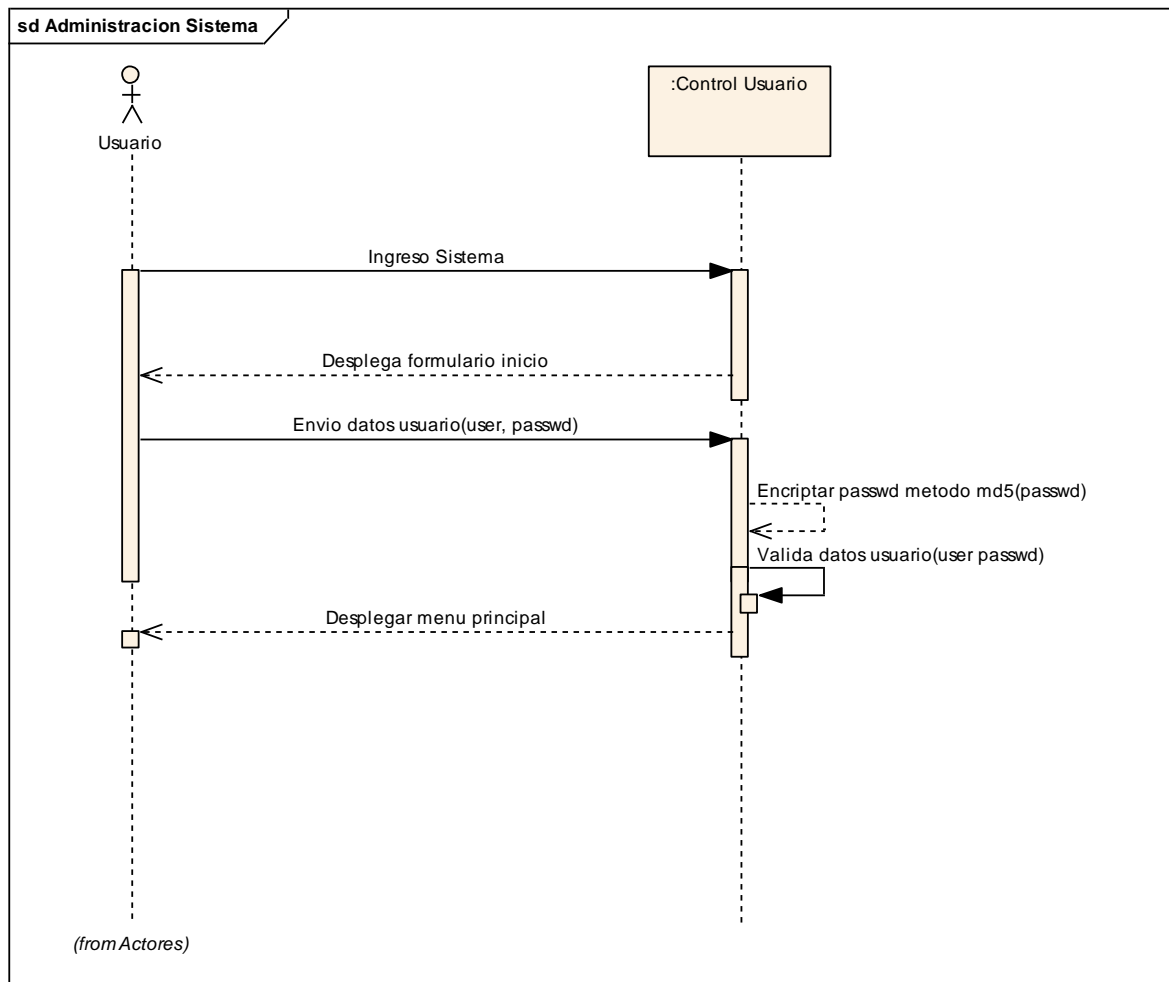


Figura 4.17: Diagrama de Secuencia Control de Usuario.

Administración de Usuarios.

Añadir Usuario.

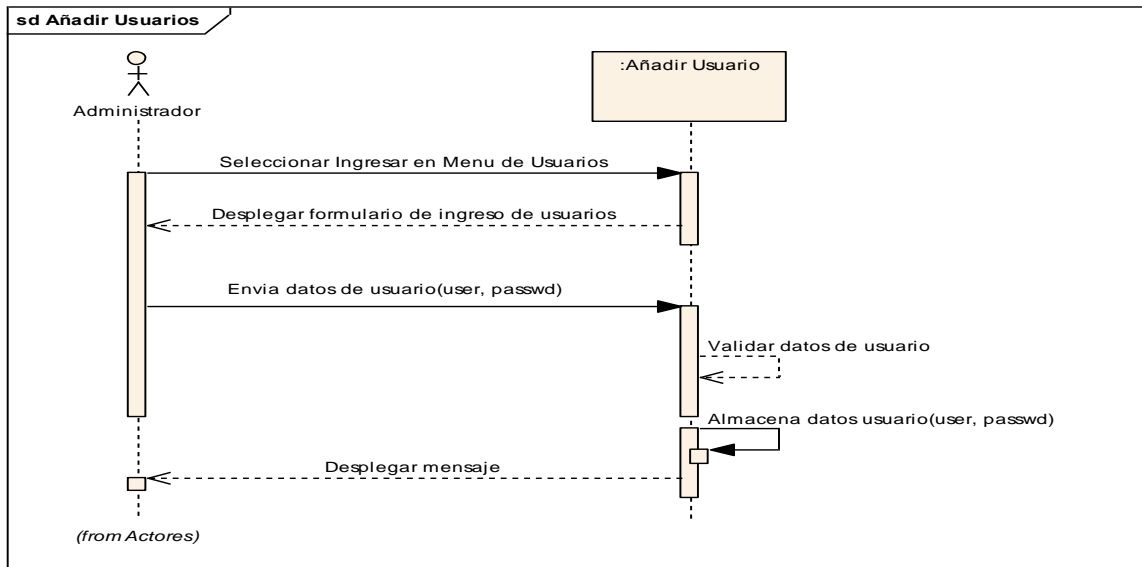


Figura 4.18: Diagrama de Secuencia Añadir Usuario.

Modificar Usuario.

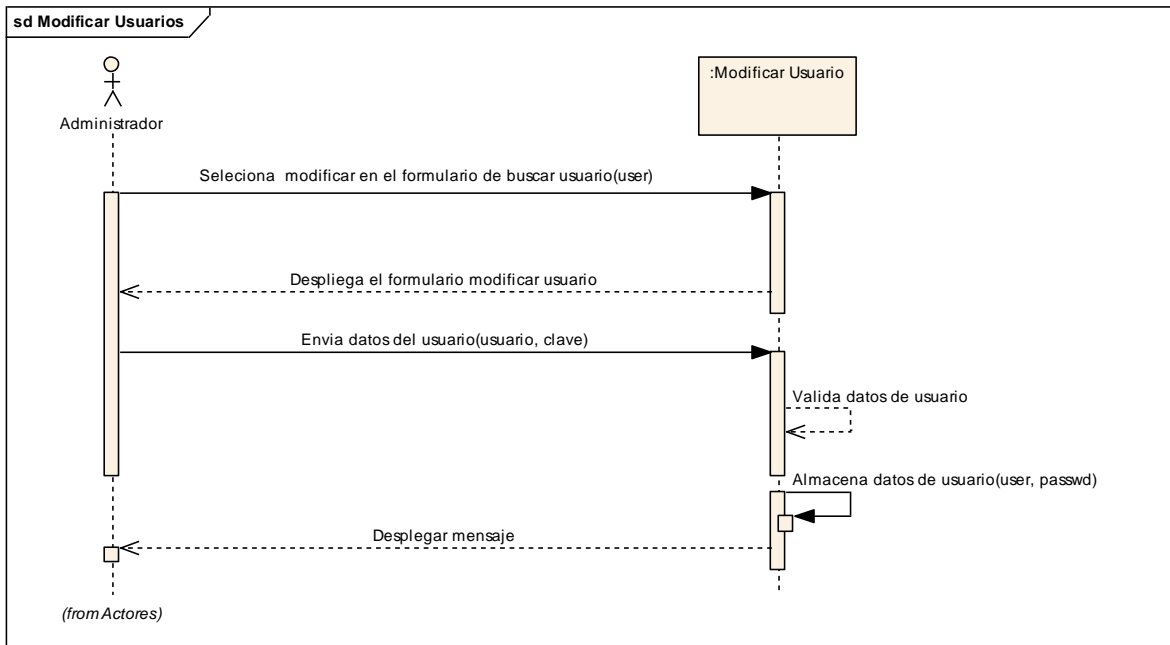


Figura 4.19 Diagrama de Secuencia Modificar Usuario.

Eliminar Usuario.

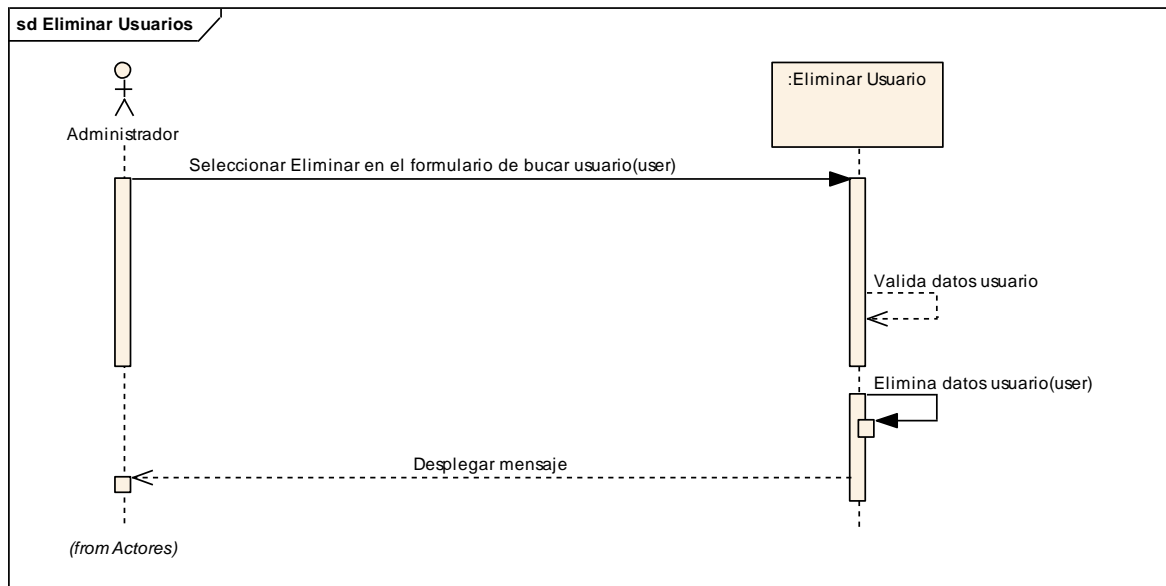


Figura 4.20: Diagrama de Secuencia Eliminar Usuario.

Administración de Clientes.

Añadir Clientes.

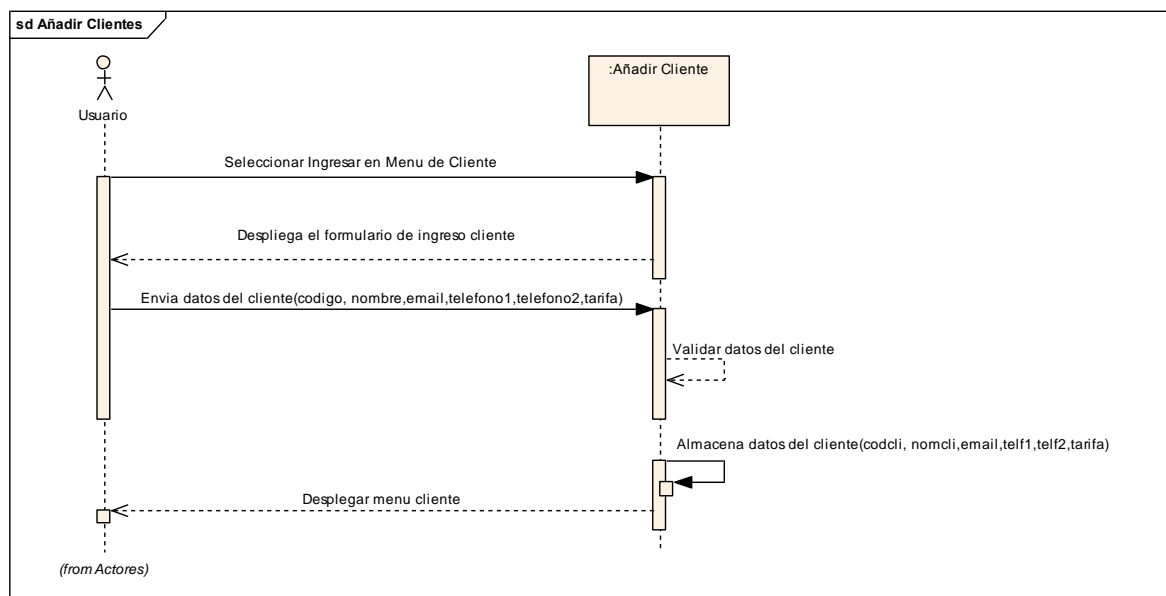


Figura 4.21: Diagrama de Secuencia Añadir Cliente.

Modificar Clientes.

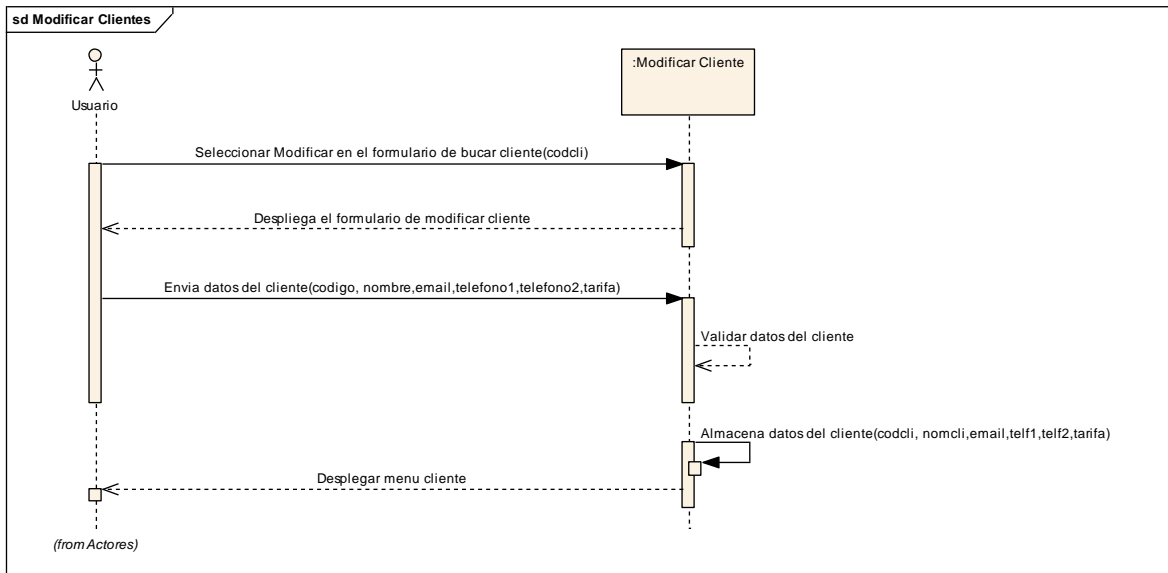


Figura 4.22: Diagrama de Secuencia Modificar Cliente.

Eliminar Clientes.

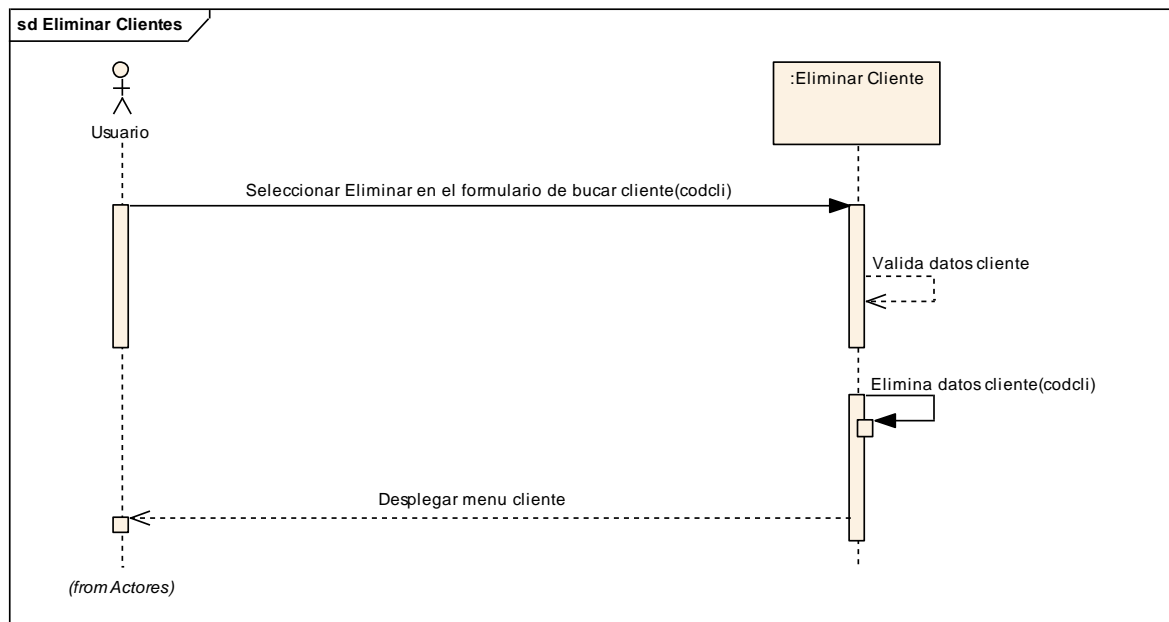


Figura 4.23: Diagrama de Secuencia Eliminar Cliente.

Reporte de Clientes.

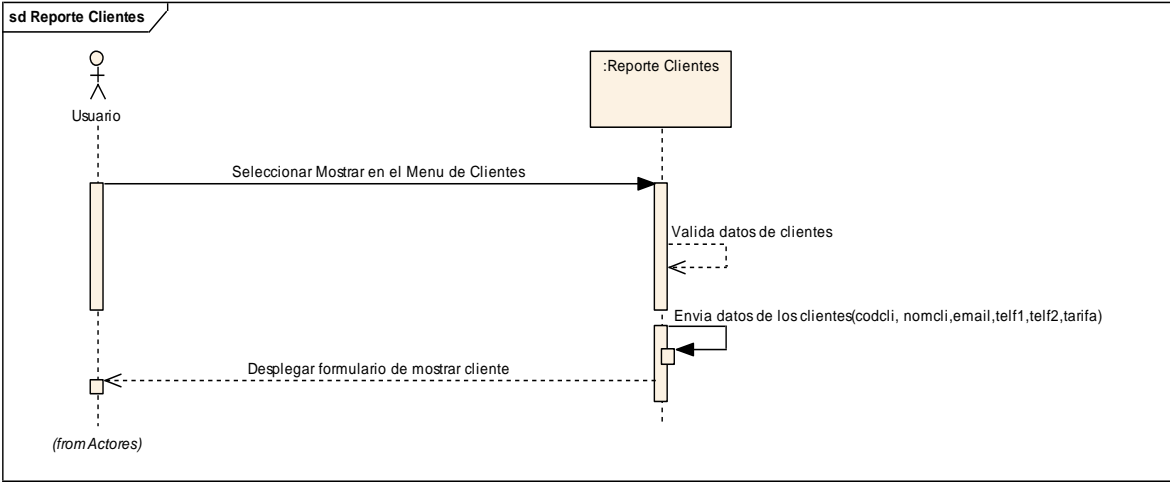


Figura 4.24: Diagrama de Secuencia Reporte Cliente.

Administración de Artículos.

Añadir Artículos.

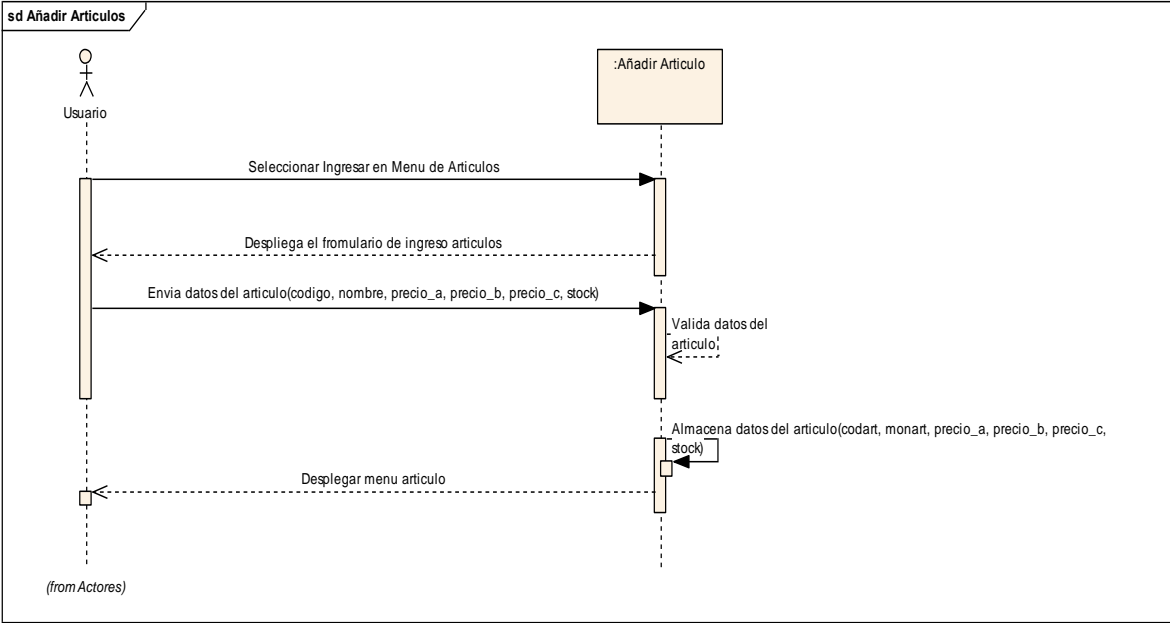


Figura 4.25: Diagrama de Secuencia Añadir Artículo.

Modificar Artículo.

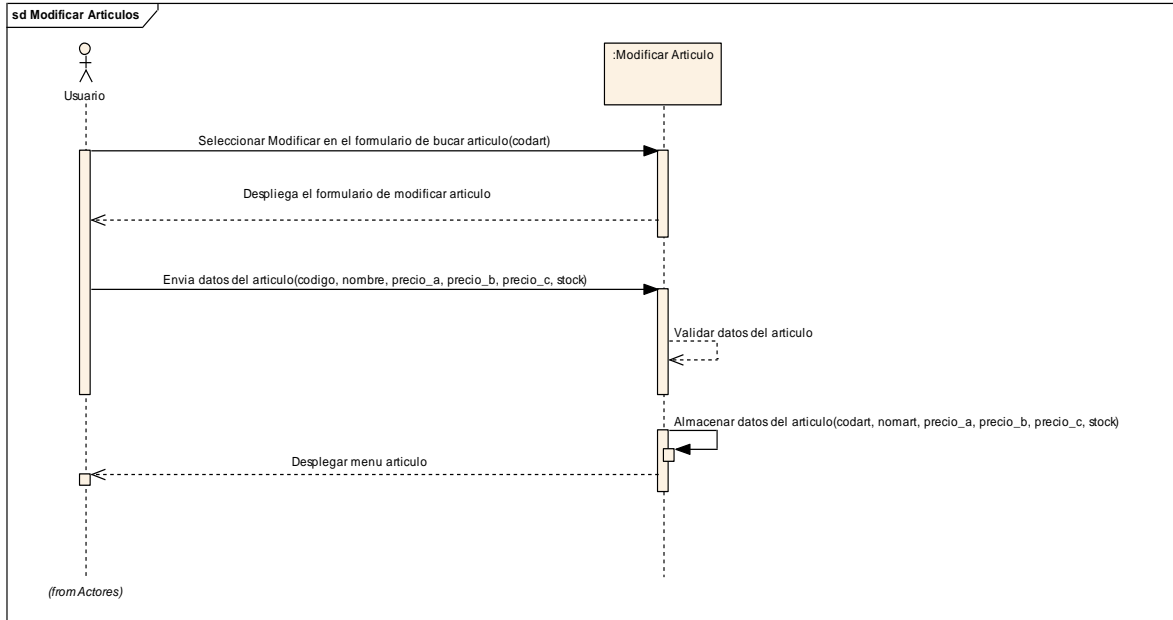


Figura 4.27: Diagrama de Secuencia Modificar Artículo.

Eliminar Artículos.

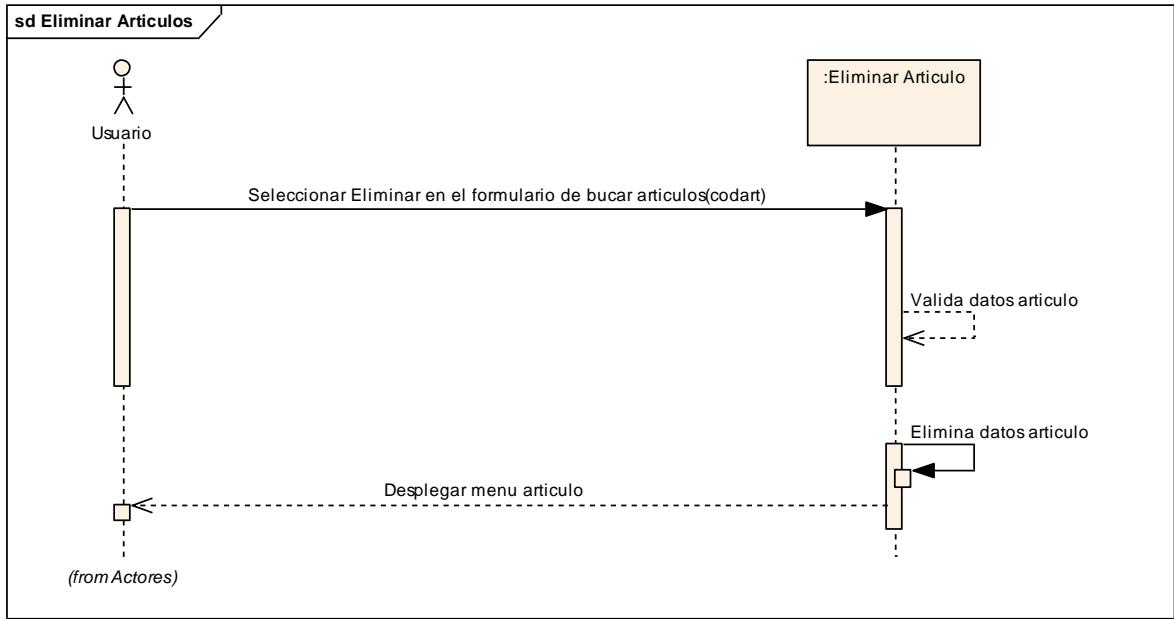


Figura 4.28: Diagrama de Secuencia Eliminar Artículo.

Reporte Artículos.

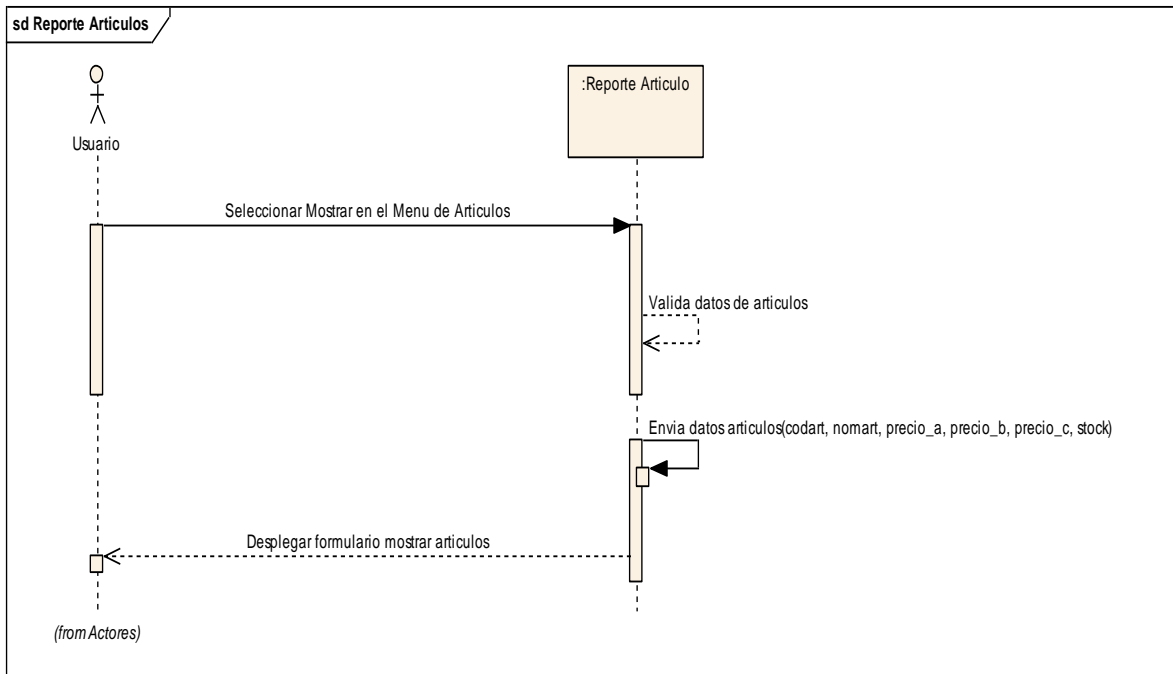


Figura 4.29: Diagrama de Secuencia Reporte Artículos.

Administración de Pedidos.

Añadir Pedido.

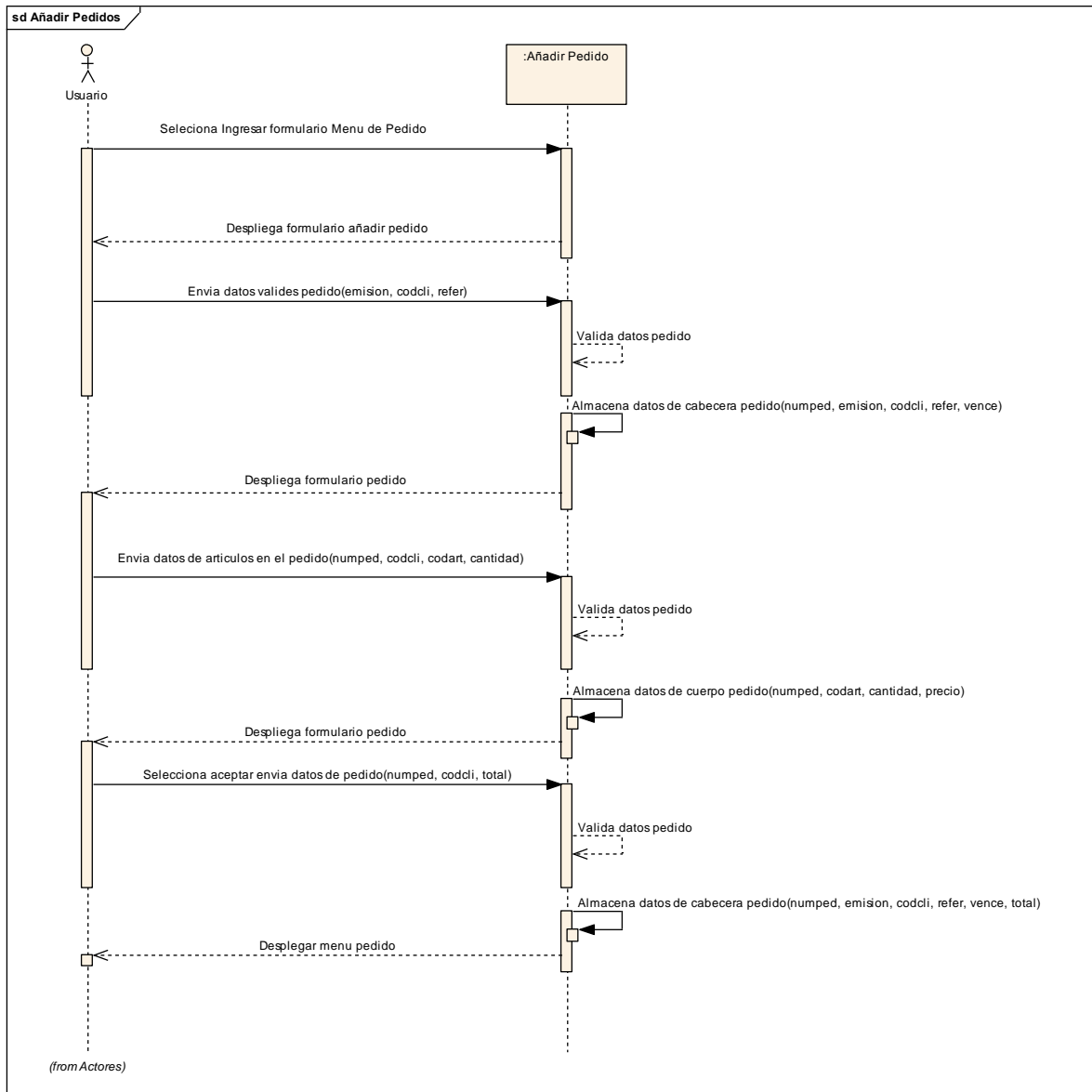


Figura 4.30: Diagrama de Secuencia Añadir Pedido.

Modificar Pedido.

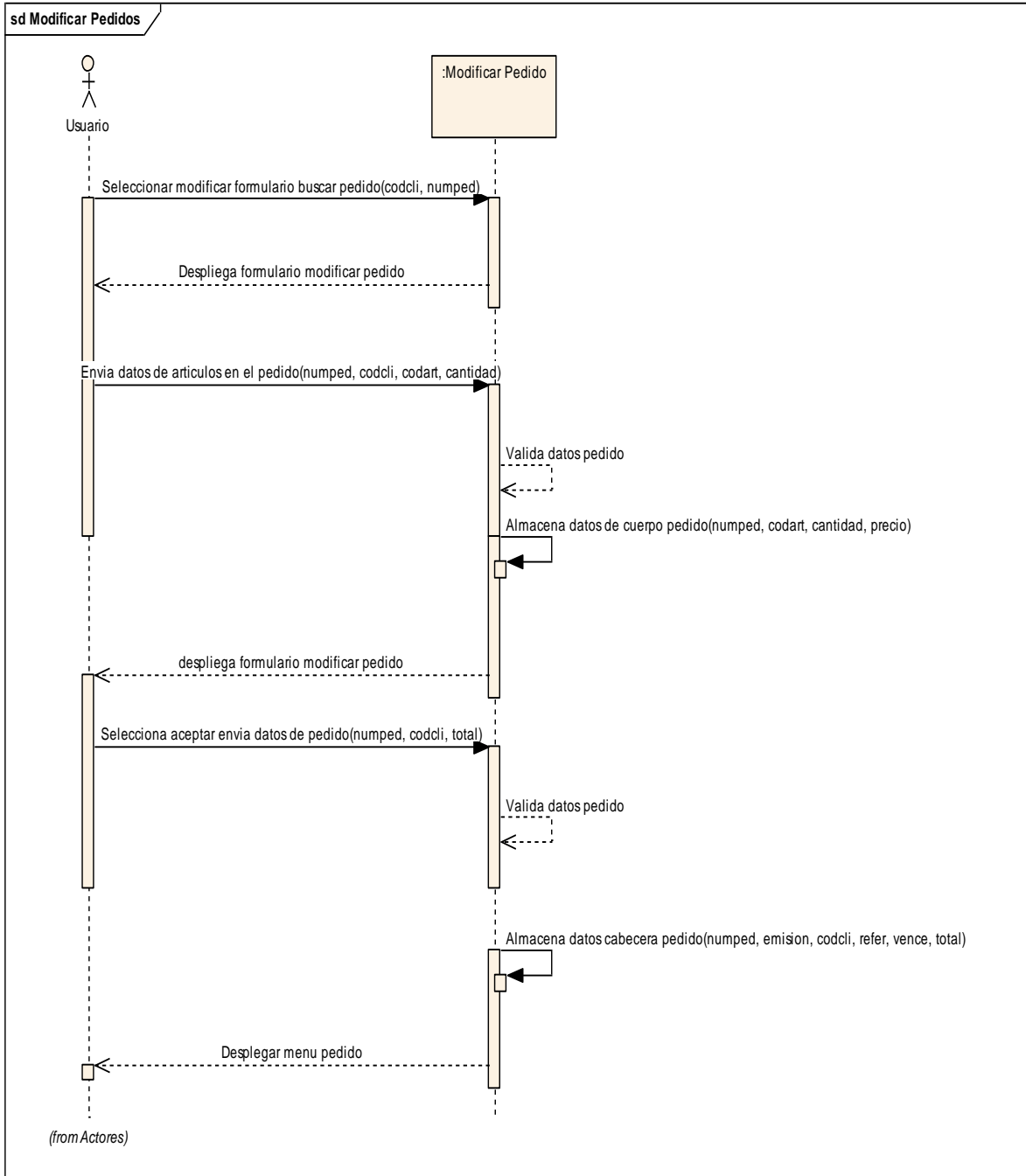


Figura 4.31: Diagrama de Secuencia Modificar Pedido.

Eliminar Pedido.

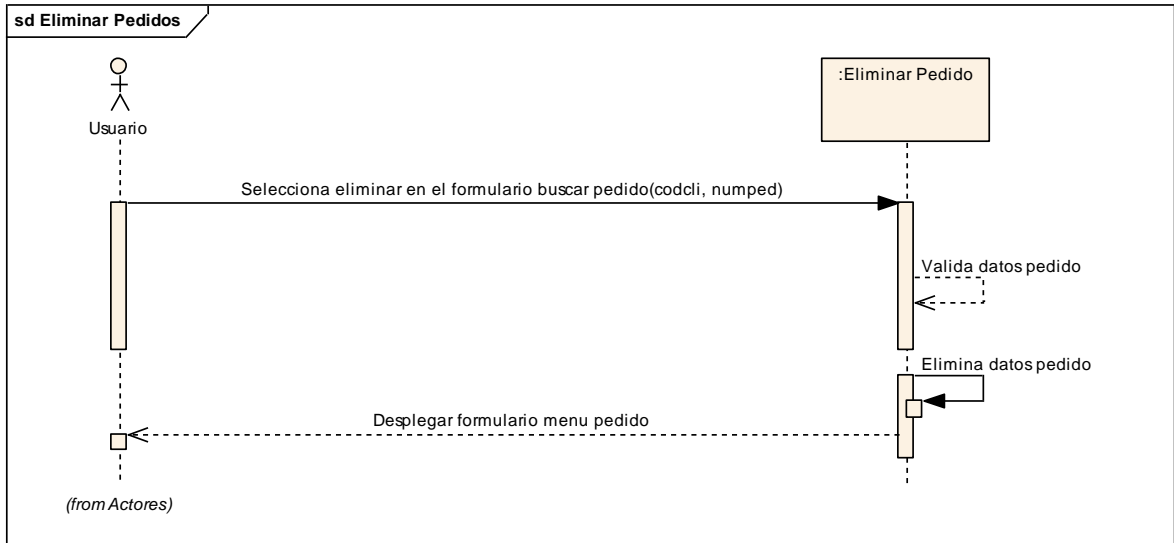


Figura 4.32: Diagrama de Secuencia Eliminar Pedido.

Administración de Saldos.

Reporte de Saldos Por Cliente.

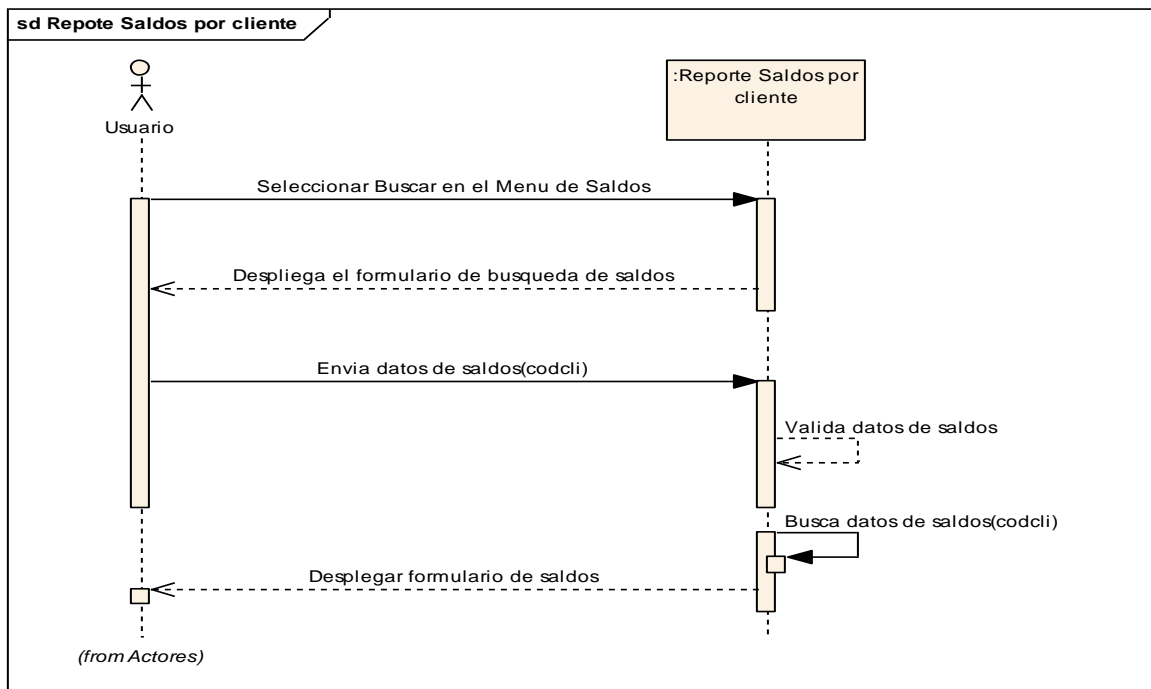


Figura 4.33: Diagrama de Secuencia Reporte Saldos por Cliente.

Reporte De Saldos.

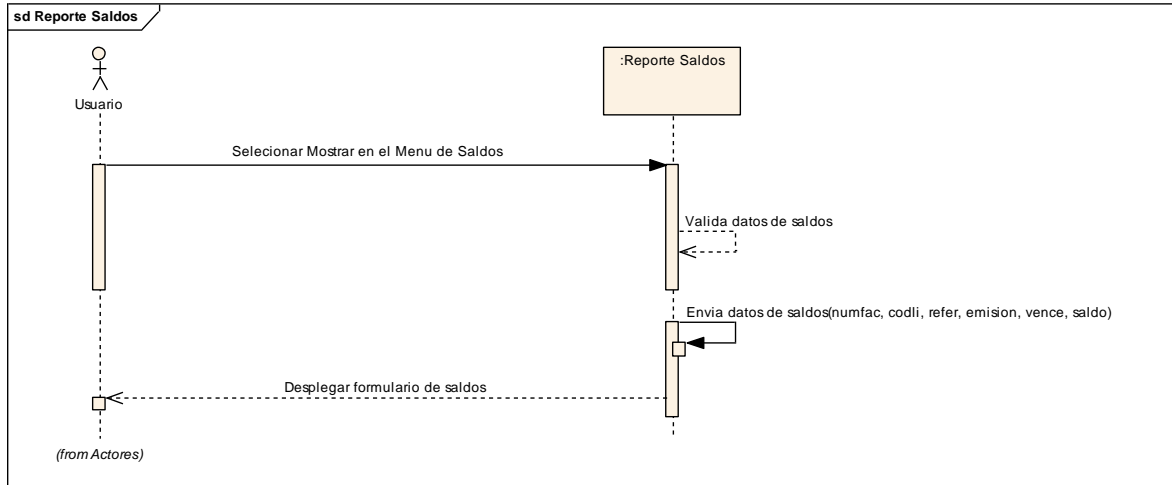


Figura 4.33: Diagrama de Secuencia Reporte Saldos.

4.3.1.3 Contratos de Operaciones.

Administración de Usuarios.

Nombre del Contrato: Añadir Usuario.

Propósito: Permite al administrador añadir un nuevo usuario (nombre de usuario y clave) en el formulario de añadir usuario.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el usuario.

Salida presenta el formulario de añadir usuario.

Precondiciones: Relación Interfaz---Administrador.

Formulario---Administrador.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Modificar Usuario.

Propósito: Permite al administrador modificar un usuario (nombre de usuario y clave) en el formulario de modificar usuario.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el usuario.

Salida presenta el formulario de modificar usuario.

Precondiciones: Relación Interfaz---Administrador.

Formulario---Administrador.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Eliminar Usuario.

Propósito: Permite al administrador eliminar un usuario (nombre de usuario) en el formulario de eliminar usuario.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el usuario.

Salida presenta el formulario de eliminar usuario.

Precondiciones: Relación Interfaz---Administrador.

Formulario---Administrador.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Control de Usuario.

Propósito: Permite al usuario ingresar al sistema (nombre de usuario y clave) en el formulario de index.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el usuario.

Salida presenta el formulario de index.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Administración Clientes.

Nombre del Contrato: Añadir Cliente.

Propósito: Permite al usuario añadir cliente (código cliente, nombre del cliente, email, telefono1, telefono2 y tarifa) en el formulario de ingresar cliente.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el cliente.

Salida presenta el formulario de ingresar cliente.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Modificar Cliente.

Propósito: Permite al usuario modificar cliente (código cliente, nombre del cliente, email, telefono1, telefono2 y tarifa) en el formulario de modificar cliente.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el cliente.

Salida presenta el formulario de modificar cliente.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Eliminar Cliente.

Propósito: Permite al usuario eliminar cliente (código cliente) en el formulario de eliminar cliente.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el cliente.

Salida presenta el formulario de eliminar cliente.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Reporte Cliente.

Propósito: Permite al usuario el reporte de clientes en el formulario de reporte cliente.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el cliente.

Salida presenta el formulario de reporte cliente.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Administración Artículos.

Nombre del Contrato: Añadir Artículo.

Propósito: Permite al usuario añadir artículo (código artículo, nombre del artículo, precio_a, precio_b, precio_c y stock) en el formulario de ingresar artículo.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el artículo.

Salida presenta el formulario de ingresar artículo.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Modificar Artículo.

Propósito: Permite al usuario modificar artículo (código artículo, nombre del artículo, precio_a, precio_b, precio_c y stock) en el formulario de modificar artículo.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el artículo.

Salida presenta el formulario de modificar artículo.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Eliminar Artículo.

Propósito: Permite al usuario eliminar artículo (código artículo) en el formulario de eliminar artículo.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el artículo.

Salida presenta el formulario de eliminar artículo.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Reporte Artículo.

Propósito: Permite al usuario el reporte de artículos en el formulario de reporte artículo.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el artículo.

Salida presenta el formulario de reporte artículo.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Administración Pedidos.

Nombre del Contrato: Añadir Pedido.

Propósito: Permite al usuario añadir pedido (número de factura, código del cliente, referencia,

emisión y vence) en el formulario de ingresar pedido.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el pedido.

Salida presenta el formulario de ingresar pedido.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Modificar Pedido.

Propósito: Permite al usuario Modificar pedido (número de factura, código del cliente) en el formulario de modificar pedido.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el pedido.

Salida presenta el formulario de modificar pedido.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Eliminar Pedido.

Propósito: Permite al usuario eliminar pedido (número de factura, código del cliente) en el formulario de eliminar pedido.

Tipo: Sistema.

Excepción: No existe sección activa.

No existe el pedido.

Salida presenta el formulario de eliminar pedido.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Administración Saldos.

Nombre del Contrato: Reporte de Saldos por Cliente.

Propósito: Permite al usuario reporte de saldos por cliente (código del cliente) en el formulario de reporte de saldos por cliente.

Tipo: Sistema.

Excepción: No existe sección activa.

No existen saldos.

Salida presenta el formulario de reporte de saldos por cliente.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.

Instancias que se eliminan.

Atributos de los objetos que se modifican.

Nombre del Contrato: Reporte de Saldos.

Propósito: Permite al usuario reporte de saldos en el formulario de reporte de saldos.

Tipo: Sistema.

Excepción: No existe sección activa.

No existen saldos.

Salida presenta el formulario de reporte de saldos.

Precondiciones: Relación Interfaz---Usuario.

Formulario--- Usuario.

Poscondiciones: Relaciones que se generan.

Instancia que se crea.
 Instancias que se eliminan.
 Atributos de los objetos que se modifican.

4.3.1.4 Diagrama de Clases.

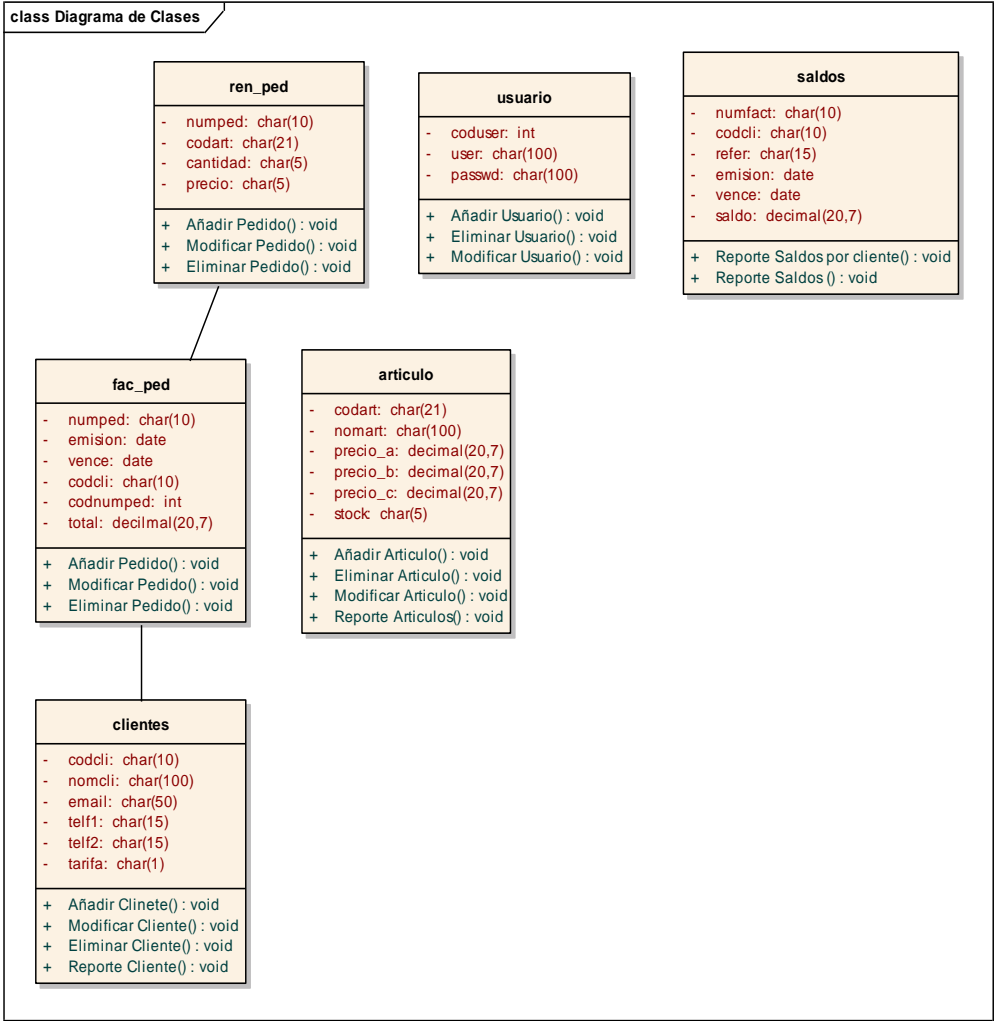


Figura 4.34: Diagrama de Clases del Sistema WAP.

4.3.1.5 Modelo Entidad Relación.

Este modelo nos permite diseñar la base de datos orientada a Mysql con la cual el sistema interactúa.

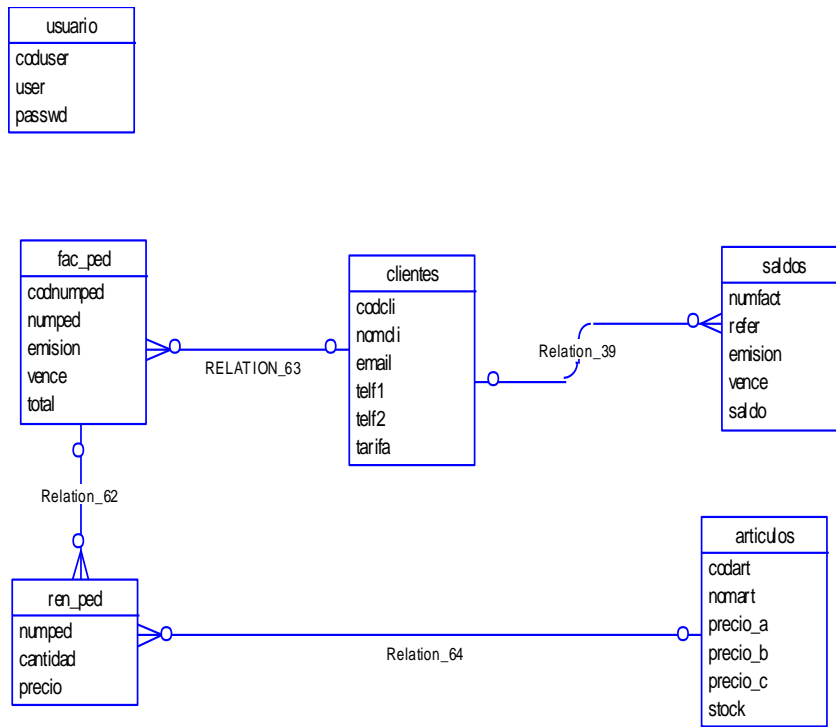


Figura 4.35: Vista Lógica del modelo Entidad Relación.

USUARIO	
CODUSER	INTEGER
USER	CHAR(100)
PASSWD	CHAR(100)

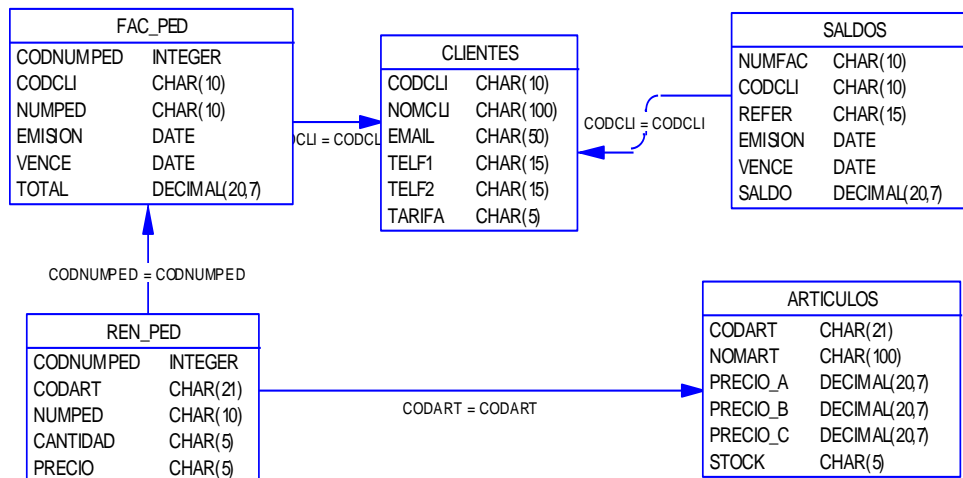
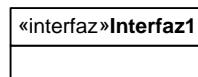


Figura 4.36: Vista Física del Modelo Entidad Relación.

4.3.2 Diseño Navegación.

Este diseño nos demuestra como funciona la navegación del sistema:



Formulario representado al usuario.



Comunicación de envió.



Comunicación de retorno.

Administración Usuario.

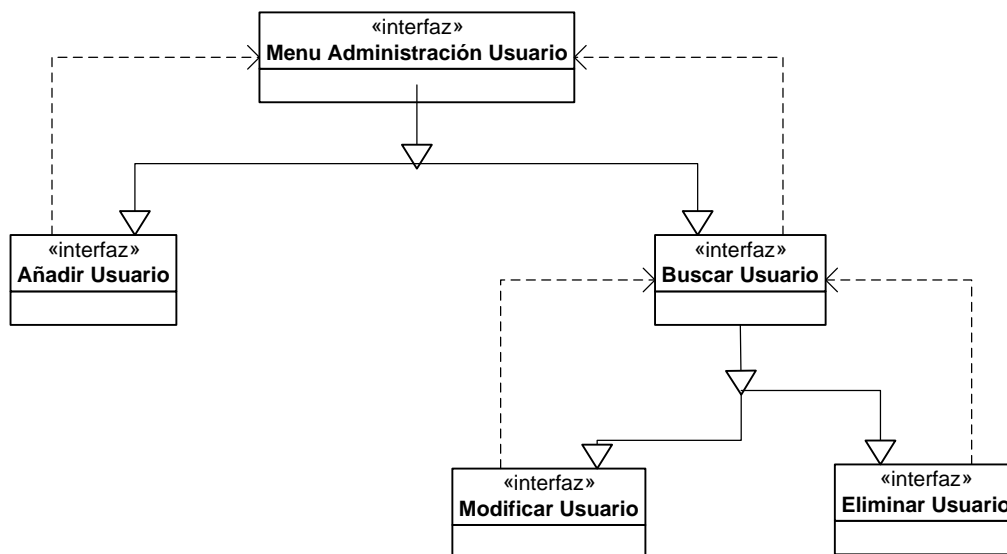


Figura 4.37: Interfaz de Manejo de Administración De Usuario.

Internases De Administración del Módulo Cartera De Clientes (Cuentas Por Cobrar) Del Sistema Administrativo Integrado FENIX.

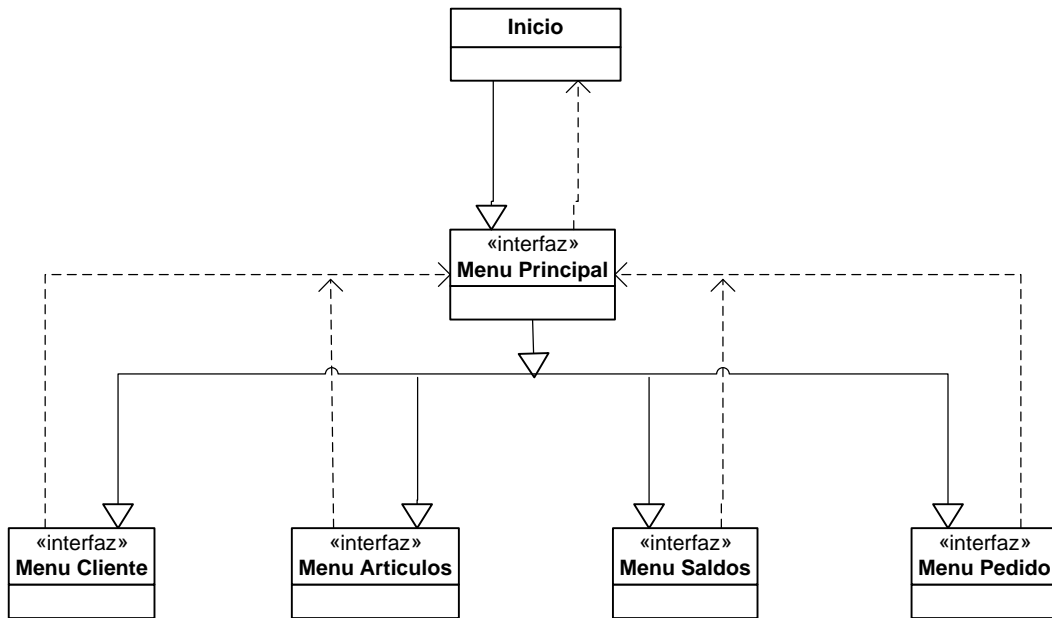


Figura 4.38: Interfaz de Manejo deL Ingreso y Menú Principal del Sistema.

Administración Cliente.

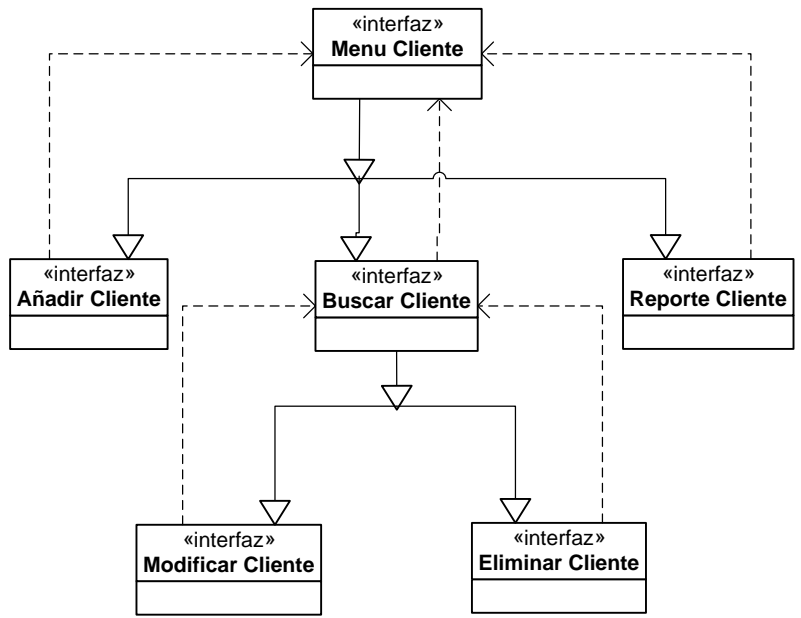


Figura 4.39: Interfaz de Manejo de Administración De Clientes.

Administración Artículo.

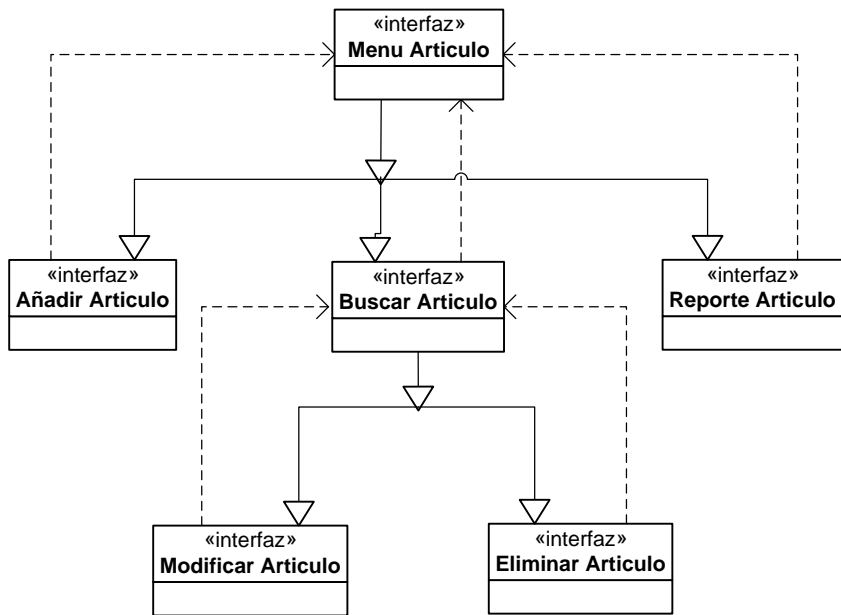


Figura 4.40: Interfaz de Manejo de Administración De Usuario.

Administración Saldos.

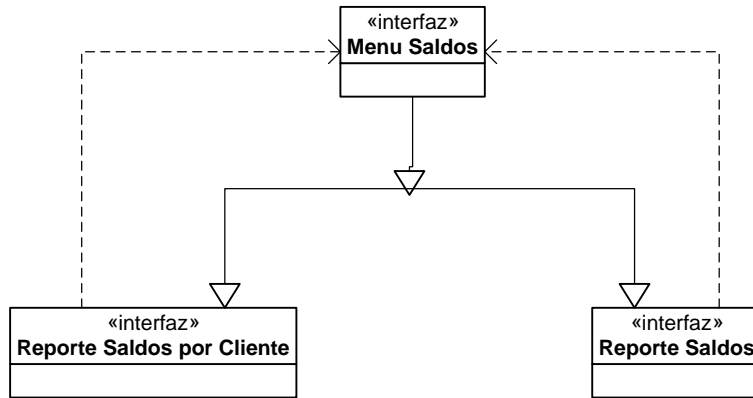


Figura 4.41: Interfaz de Manejo de Administración De Usuario.

Administración Pedido.

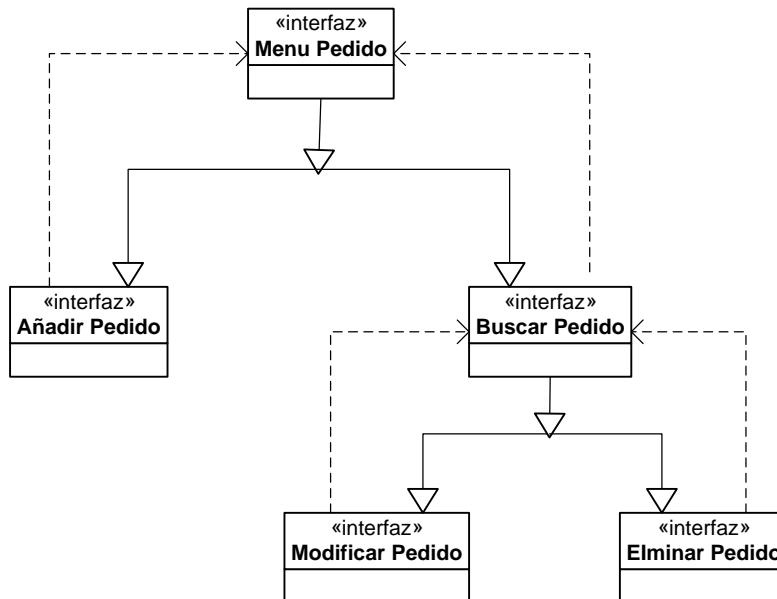


Figura 4.42: Interfaz de Manejo de Administración De Usuario.

4.3.3 Diseño Interfaz.

Este diseño nos demuestra las pantallas que presenta el sistema al usuario y al administrador:



Figura 4.43: Ingresando Al Sistema. Emulador WAP.



Figura 4.44: Menús Del Sistema. Emulador WAP.



Figura 4.45: Registro De Clientes. Emulador WAP.



Figura 4.46: Búsqueda y Validación Del Cliente. Emulador WAP.

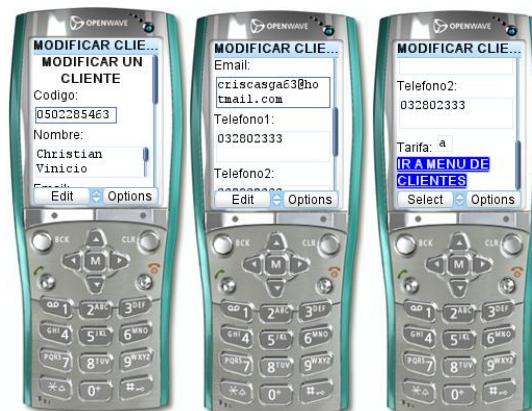


Figura 4.47: Modificación y Validación Del Cliente. Emulador WAP.



Figura 4.48: Reporte De Los Clientes. Emulador WAP.



Figura 4.49: Registro De Artículos. Emulador WAP.



Figura 4.50: Búsqueda y Validación De Artículos. Emulador WAP.



Figura 4.51: Modificación y Validación De Artículos. Emulador WAP.



Figura 4.52: Reporte De Los Artículos. Emulador WAP.



Figura 4.52: Validación Del Ingreso Del Pedido. Emulador WAP.

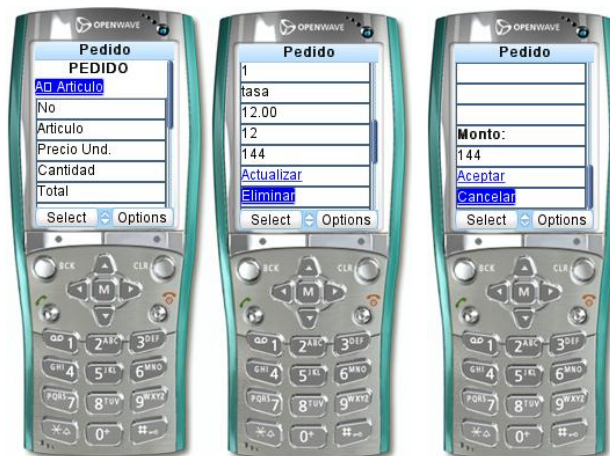


Figura 4.53: Validación Del Pedido. Emulador WAP.



Figura 4.54: Búsqueda y Validación Del Pedido. Emulador WAP.



Figura 4.55: Modificación y Validación Del Pedido. Emulador WAP.



Figura 4.55: Reporte De Los Saldos Por Un Cliente. Emulador WAP.



Figura 4.56: Reporte De Los Saldos Por Un Cliente. Emulador WAP.

4.4 CODIFICACIÓN.

La codificación del sistema fue realizado de acuerdo a las especificaciones descritas por el usuario en las etapas de análisis y diseño del sistema, los script creados para el sistema están realizados con un lenguaje de programación wml con php en la herramienta llamada Macromedia Dreamweaver MX.

Ejemplo de bloque de código wml:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<card>
<p align="center" mode="wrap">
Telefonía Móvil
</p>
</card>
</wml>
```

- Este bloque del programa debe incluirse siempre:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
```

"http://www.wapforum.org/DTD/wml_1.1.xml ">

- Aquí se define la versión como la definición XML del lenguaje a utilizar.

Y el código que esta entre<wml>...</wml> es a lo que se le llama la baraja, la cual se subdivide en cartas <card>...</card>, dentro de las cartas pueden contener elementos como párrafos <p>...</p> los cuales pueden definirse ciertas propiedades.

Como center = Parrafo centrado

Modo wrap = Modo de presentación envuelto, e cual garantiza que el texto de ser muy largo severa en la línea siguiente.

4.5 IMPLEMENTACIÓN.

La implementación del sistema fue realizado de acuerdo a las especificaciones descritas en las etapas de análisis y diseño del sistema, los script creados para el sistema están en la carpeta tesis del disco provisto en la tesis.

4.5.1 Prerrequisitos Para La Instalación.

Para instalar el sistema es necesario conocer los requisitos previos suficientes y necesarios para la instalación, es recomendable usar las versiones de software estipuladas en este documento ya que el sistema ha sido testeado únicamente con estas versiones.

Para instalar el sistema es necesario:

- Windows XP Profesional.
- Apache Web Server (Apache_1.3.34-Mod_SSL_2.8.25-Openssl_0.9.8a-Win32).
- Mysql.
- Php.

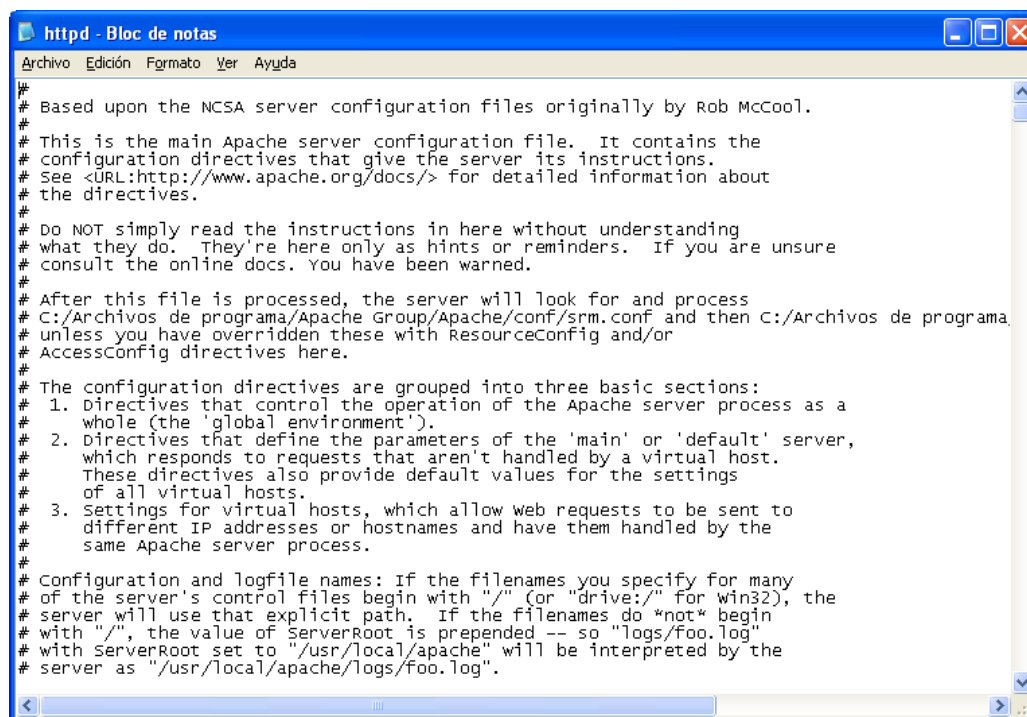
4.5.2 Instalación y Configuración del APACHE.

Internet se compone de miles de servidores que almacenan las páginas que vemos a los que acceden los clientes. El sistema seguido por WAP no es la diferencia.

El servidor es el mismo con diferente configuración pero ahora los dispositivos son móviles para que la aplicaron se pueda ver.

1. Instalar el servidor Apache, para esto podemos descargar el archivo de instalación de apache en www.apache.org o en el disco de instalación del sistema, el archivo de instalación es **Apache_1.3.34-Mod_SSL_2.8.25-Openssl_0.9.8a-Win32**.
2. Detectar el archivo de configuración del Apache **httpd.conf**, el cual se encuentra en un subdirectorio **conf** y modificarlo por ejemplo:

c:\Apache\conf



```
httpd - Bloc de notas
Archivo Edición Formato Ver Ayuda
#
# Based upon the NCSA server configuration files originally by Rob McCool.
#
# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See <URL:http://www.apache.org/docs/> for detailed information about
# the directives.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# After this file is processed, the server will look for and process
# C:/Archivos de programa/Apache Group/Apache/conf/srm.conf and then C:/Archivos de programa
# unless you have overridden these with ResourceConfig and/or
# AccessConfig directives here.
#
# The configuration directives are grouped into three basic sections:
# 1. Directives that control the operation of the Apache server process as a
# whole (the 'global environment').
# 2. Directives that define the parameters of the 'main' or 'default' server,
# which responds to requests that aren't handled by a virtual host.
# These directives also provide default values for the settings
# of all virtual hosts.
# 3. Settings for virtual hosts, which allow web requests to be sent to
# different IP addresses or hostnames and have them handled by the
# same Apache server process.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for win32), the
# server will use that explicit path. If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/foo.log"
# with ServerRoot set to "/usr/local/apache" will be interpreted by the
# server as "/usr/local/apache/logs/foo.log".
```

Figura 4.57: Archivo de configuración del servidor Apache.

Dentro del archivo **httpd.conf**, tenemos una serie de valores que es conveniente modificar.

- **ServerRoot “directorio”**: Aquí tenemos el directorio donde esta instalado el Apache.

ServerRoot "C:/Apache"

- **Port “numero”**: Aquí tenemos el puerto por el cual se van a realizar las conexiones.

Port 80

- **ServerAdmin “email”**: Dirección de correo del administrador del servidor web (webmaster). Se usa para que el administrador reciba correos de clientes diciéndole los fallos que hay en sus páginas.

ServerAdmin admin@localhost

- **ServerName “nombre”**: nos muestra el nombre de la maquina donde tenemos instalado el apache.

ServerName localhost

- **DocumentRoot**: Aquí tenemos el directorio donde se almacena las paginas que proporcionara el servidor Apache.

DocumentRoot "C:/Apache/htdocs"

- **DirectoryIndex “archivo”**: Aquí tenemos el archivo índice que se ejecuta automáticamente al abrir el directorio.

**DirectoryIndex index.html index.htm index.php index.php4 index.php3 index.cgi index.pl
index.html.var index.phtml index.wml**

Para que el servidor Apache pueda interpretar paginas WAP se añade estas líneas al final del **httpd.conf**.

```
#MINES tipo para WAP.  
AddType text/vnd.wap.wml wml  
AddType image/vnd.wap.wbmp wbmp
```



```
AddType text/vnd.wap.wmlscript wmls  
AddType application/vnd.wap.wmlc wmlc  
AddType application/vnd.wap.wmlscriptc wmls
```

3. Configurar Apache+SSL en Win32.

Cambia al menos los siguientes parámetros en(Apache-dir)/conf/httpd.conf:

- Port 80 to # Port 80 (Pónlo como comentario; Port no es necesario, Listen lo sobrescribe más tarde).
 - (Si no es además de IIS) Listen 80.
 - Listen 443 (Así el servidor escucha en el puerto standard SSL).
4. Instalo el Win32OpenSSL-0_9_8e(2).
 5. Copia los archivos ejecutables (*.exe, *.dll, *.so) desde la distribución descargada de apache-mod_ssl a tu directorio de instalación original de Apache (recuerda detener primero Apache y NO sobrescribir tus archivos de configuración modificados).
 6. Encuentra las directivas LoadModule en tu archivo httpd.conf y añade esto después de la última, según el nombre de archivo que viene con la distribución:

```
LoadModule ssl_module modules/mod_ssl.so
```

7. En versiones recientes de la distribución, podría ser necesario añadir también después de las líneas AddModule:

```
AddModule mod_ssl.c
```

8. Añade lo siguiente al final del httpd.conf:

```
SSLMutex sem  
SSLRandomSeed startup builtin  
SSLSessionCache none  
SSLLog logs/SSL.log  
SSLLogLevel info
```

Más tarde puedes cambiar "info" a "warn" si todo funciona correctamente

<VirtualHost localhost:443>

SSLEngine On

SSLCertificateFile conf/ssl/adsecuador.cert

SSLCertificateKeyFile conf/ssl/adsecusdor.key

</VirtualHost>

4.5.3 Creando un certificado.

Para crear un certificado se procede de la siguiente manera:

1. Se ingresa la carteta **C:\OpenSSL\bin** y ejecuta el archivo **openssl.exe** se la aparece este pantalla:
2. Crea una petición de firma de certificado y una llave privada. Cuando sea pedido "Common Name (pe, nombre de dominio de tu sitio Web)", dá el nombre de dominio exacto de tu servidor Web.

req -config openssl.cnf -new -out adsecuador.csr

```
C:\OpenSSL\bin\openssl.exe
OpenSSL> req -config openssl.cnf -new -out adsecuador.csr
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
...+++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ec
State or Province Name (full name) [Some-State]:cotopaxi
Locality Name (eg, city) []:latacunga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:adsecuador
Organizational Unit Name (eg, section) []:adsecuador
Common Name (eg, YOUR name) []:admin
Email Address []:adsecuador@adsecuador.com

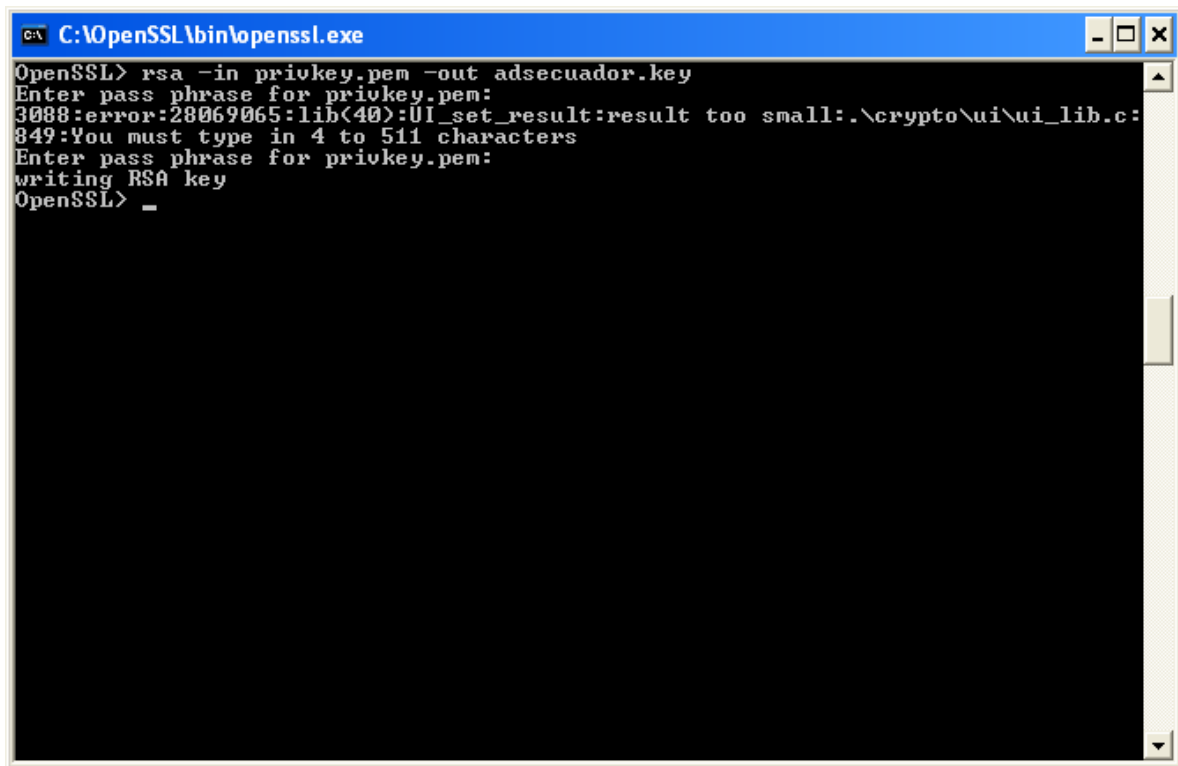
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:prueba
An optional company name []:adsecuador
OpenSSL> _
```

Figura 4.58: Pantalla De Creación de Certificado.

3. Remueve la contraseña de la llave privada. Se debe entender que significa esto: **adsecuador.key** debe ser legible solamente por el servidor y el administrador.

Debes suprimir el archivo **.rnd** porque contiene información entrópica para crear la llave y podría ser usada para ataques criptográficos contra tu llave privada.

rsa -in privkey.pem -out adsecuador.key



```
C:\OpenSSL\bin\openssl.exe
OpenSSL> rsa -in privkey.pem -out adsecuador.key
Enter pass phrase for privkey.pem:
3088:error:28069065:lib(40):UI_set_result:result too small:.\crypto\ui\ui_lib.c:
849:You must type in 4 to 511 characters
Enter pass phrase for privkey.pem:
writing RSA key
OpenSSL> _
```

Figura 4.59: Remueve Contraseña en Creación de un Certificado.

Crea un certificado con firma-propia que puede ser usado hasta que obtengas uno "real" uno de una autoridad certificada. (El cual es opcional; si conoces tus usuarios, puedes decirles que instalen el certificado en sus exploradores).

x509 -in adsecuador.csr -out adsecuador.cert -req -signkey adsecuador.key -days 365

```
C:\OpenSSL\bin\openssl.exe
OpenSSL> x509 -in adsecuador.csr -out adsecuador.cert -req -signkey adsecuador.ke
ey -days 365
Loading 'screen' into random state - done
Signature ok
subject=/C=ec/ST=cotopaxi/L=latacunga/O=adsecuador/OU=adsecuador/CN=admin/emailA
ddress=adsecuador@adsecuador.com
Getting Private key
OpenSSL> _
```

Figura 4.60: Expedición de Tiempo de un Certificado.

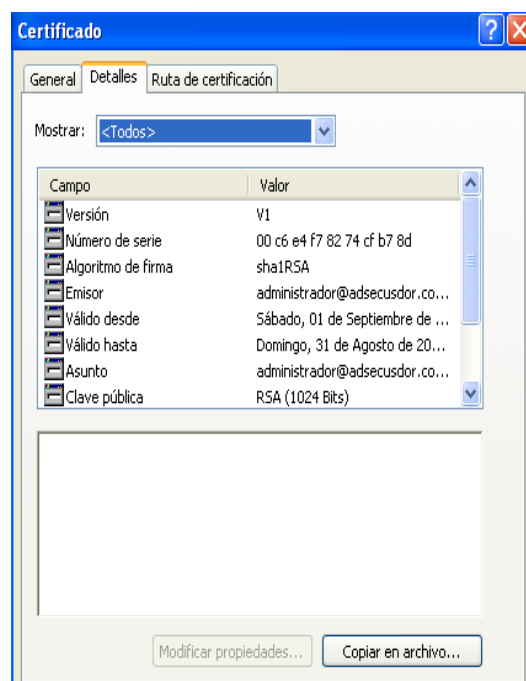


Figura 4.61: Certificado Creado.

4.5.4 Instalación y Configuración del PHP.

Para la instalación de php es necesario descargar el instalable desde www.php.net o usar el instalable contenido en el disco de instalación del sistema.

La versión del php es **php-4.3.4-Win32**.

Se crea una carpeta en la raíz llamada php, dentro de esta existen dos archivos un **php4ts.dll** el cual debe ser copiado y pegado en la carpeta **C:\WINDOWS\system32** y el archivo php.ini-recommended debe ser copiado a la carpeta **C:\WINDOWS** cambiar el nombre por **php.ini**.

En el archivo del apache httpd.conf añadimos las siguientes líneas al final.

```
ScriptAlias /php/ "c:/php/"  
AddType application/x-httpd-php .php  
Action application/x-httpd-php "/php/php.exe"
```

Por último creamos un archivo con el nombre de **info.php** con el siguiente código:

```
<?php phpinfo() ?>
```

Colócalo en el directorio de documentos de Apache y llámalo desde el navegador. Si lo hemos hecho todo bien nos saldrá una página con todas las variables de PHP.

4.5.5 Instalación y Configuración de Mysql.

Para instalar Mysql es necesario descargar el instalable desde www.mysql.com o usar el instalable contenido en el disco de instalación del sistema.

La versión de Mysql es mysql-4.0.17-win con su respectivo ODBC MyODBC-3.51.06.

La base de datos será llamada tesis, ya que así está descrito en los archivos de configuración del sistema, en el disco de instalación se encuentra el script con la base de datos, el archivo es.

```
tesis_database.sql
```

4.5.6 Instalación del Sistema.

Para instalar el sistema es necesario copiar la carpeta **tesis** hacia la dirección de ejecución de Apache, normalmente es:

C:\Apache\htdocs

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones.

Como conclusiones se puede decir:

- La creación de un sistema orientado a Tecnología WAP es posible realizarlo mediante herramientas de código abierto de fácil acceso.
- La creación del sistema permite a los usuarios de dispositivos móviles contar en cualquier parte del mundo con dicho sistema, con el cual podrán agilizar sus actividades de comercio en una forma más rápida y confiable.
- Desde el punto de vista corporativo las empresas podrán contar con una herramienta que permita acceder a su información sin necesidad de permanecer on-line, pudiendo de forma inmediata dar información instantánea.
- El uso de una interfase gráfica por medio de un servidor Web como es Apache, permite que el sistema cuente con un nivel de manejo orientado a lo que es la Tecnología WAP y ser usado por personas con un conocimiento amplio de redes.
- La seguridad en el entorno móvil en el acceso de Internet a través de dispositivos móviles se encuentra en un estado de crecimiento, por lo cual se a realizado la implementación de una seguridad a la aplicación utilizando encriptación método md5 e instalando un certificado al servidor WAP.

5.2 Recomendaciones.

Como recomendaciones se puede decir:

- Investigar el grado de conocimiento sobre Tecnología WAP en el área de Sistemas e Informática antes de iniciar un proyecto de desarrollo y migración; y de acuerdo con el resultado iniciar una capacitación sobre la configuración y manejo del mismo.
- Incrementar la difusión y la formación de WAP ya que es hoy por hoy una interesante tecnología para el desarrollo empresarial e industrial a nivel mundial.
- Para los nuevos desarrolladores de WAP no confiarse que el script generado corra igual en un dispositivo móvil como en el emulador.


- La aplicación puede ser desarrollada tanto como en plataforma de Windows como la Linux, todo depende si se puede configurar un servidor Web Apache no importa la versión.

ANEXOS.

6.1 Manual de Administrador.

El sistema consta de esta primera parte de un modulo que permite crear modificar o eliminar a los respectivos usuarios por parte de un administrador.

Si se encuentra en el servidor, para ejecutar el sistema es necesario usa la siguiente línea de conexión.

Dirección  http://localhost/administracion_usuario.php

Se despliega la ventana de menú de administración de usuario en el cual puede elegir:

- Ingresar nuevo usuario.
- Buscar usuario.

Administración de Usuarios

[INGRESAR NUEVO USUARIO](#)

[BUSCAR USUARIO](#)

Creación de nuevos usuarios.

Para la creación de un nuevo en el sistema de un clic sobre “Ingresar un nuevo Usuario”:

[INGRESAR NUEVO USUARIO](#)

El sistema despliega la ventana de añadir nuevo usuario con los datos necesarios para el ingreso.

Añadir Nuevo Usuario

Usuario:	<input type="text"/>
Clave:	<input type="text"/>
Confirme Clave:	<input type="text"/>
<input type="button" value="Ingresar Nuevo Usuario..."/>	<input type="button" value="Reset"/>

[Ir Menu Usuario](#)

El campo Usuario define el nombre del usuario que se asigna al sujeto, de igual manera el campo Clave define el password que será asignado, el campo de Confirmación Clave confirma el password asignado, esto permite controlar el ingreso al sistema en los dispositivos móviles.

Al seleccionar el botón “Ingresar Nuevo Usuario...”

Se almacena el usuario en la base de datos.

Al Seleccionar el botón "Reset" permite resetear los campos en caso de un mal ingreso de datos.

Reset

O al asignar el fash text "Ir Menú Usuario" nos permite retornar a la ventana de administración de usuarios.

[Ir Menu Usuario](#)

Modificación, Eliminación de usuarios existentes.

Para la modificación o eliminación de un usuario en el sistema de un clip sobre "Buscar Usuario":

[BUSCAR USUARIO](#)

El sistema despliega la ventana de búsqueda de usuario con los datos necesarios para el ingreso.

Buscar Usuario

Nombre del Usuario:

Buscar Reset

[Ir Menu Usuario](#)

El campo Nombre del Usuario define el nombre del usuario que se asigno al sujeto existente en la base de datos, esto permite controlar la modificación de datos de los usuarios para su mejor funcionamiento al sistema en los dispositivos móviles.

Al Seleccionar el botón "Reset" permite resetear los campos en caso de un mal ingreso de datos.

Reset

Al seleccionar el botón “Buscar”

Buscar

Si el usuario existe despliega en la misma ventana con la información básica del usuario en la cual nos permite modificar o eliminar al usuario.

Buscar Usuario

Nombre del Usuario:

Buscar Reset

admin [Modificar](#) [Eliminar](#)

[Ir Menu Usuario](#)

Al asignar el fash text “Eliminar” nos permite eliminar a usuarios existentes en la base de datos.

[Eliminar](#)

Al asignar el fash text “Modificar” nos permite ir a la ventana de modificación de usuarios.

[Modificar](#)

Modificar Datos de Usuario

Usuario:	<input type="text" value="admin"/>
Clave:	<input type="password" value="•••••"/>
Confirme Clave:	<input type="password"/>
<input type="button" value="Modificar"/>	<input type="button" value="Reset"/>

El campo Usuario nos muestra el nombre del usuario que se asigno al sujeto existente en la base de datos, también nos despliega en el campo clave el dato del password el cual puede ser modificado y para modificar se lo reescribe y se confirma el password en el campo de confirmación de clave, esto permite modificar la clave del usuario en caso que el se aya olvidado o desee actualizar.

Al asignar el fash text “Ir Menú Usuario” nos permite retornar a la ventana de administración de usuarios.

[Ir Menu Usuario](#)

6.2 Manual de Usuario.

El sistema consta de esta segunda parte de un modulo orientado a dispositivos móviles que permite crear modificar o eliminar clientes, artículos, realizar, modificar o eliminar pedidos y permite reportar saldos de los clientes a los respectivos usuarios registrados en el sistema.

Si se encuentra en el celular, para ejecutar el sistema es necesario usa la siguiente línea de conexión.

<http://190.11.13.47/index.wml>

Se despliega el cards “la bienvenida del sistema” para poder ingresar:



Al seleccionar en opciones “Ok” se despliega el cards de inicio.



Ingresamos el usuario y la clave respectiva para su verificación correspondiente y comenzar la navegación dentro del sistema.

Al seleccionar en opciones "Ok" se despliega el cards del Menú Principal siempre y cuando el usuario y la clave correspondan a los registrados en la base de datos.



El cards de menú principal nos muestra las siguientes opciones de navegación.

- Clientes.
- Artículos.
- Saldos.
- Pedidos.

Los cuales nos permiten ingresar a los correspondientes cards de submenús.



En los cuales existen opciones de navegación tales como:

Menú Clientes:

- Ingresar: permite desplegar el cards ingresar cliente.
- Buscar: permite desplegar el cards buscar cliente.
- Mostrar: permite desplegar el cards mostrar clientes.

- Salir: permite desplegar el cards de menú principal.

Menú Artículos.

- Ingresar: permite desplegar el cards ingresar artículo.
- Buscar: permite despliega el cards buscar artículo.
- Mostrar: permite despliega el cards mostrar artículos.
- Salir: permite despliega el cards de menú principal.

Menú Saldos.

- Buscar: permite desplegar el cards buscar saldos.
- Mostrar: permite desplegar el cards mostrar saldos.
- Salir: permite desplegar el cards menú principal.

Menú Pedidos.

- Ingresar: permite desplegar el cards valides pedido.
- Buscar: permite desplegar el cards buscar pedido.
- Salir: permite desplegar el cards menú principal.

Administración De Clientes.

Creación de nuevos clientes.

Despliega el cards ingresar cliente con los campos necesarios para el ingreso.



El campo código define el código del cliente que se le asigna al sujeto, de la misma manera el nombre define el nombre completo, email el email, telefono1 y telefono2 los correspondientes números de teléfono y la tarifa la cual define el modo de nivel del cliente, esto permite controlar todo el movimiento de transacciones de dicho cliente.

Buscar clientes.

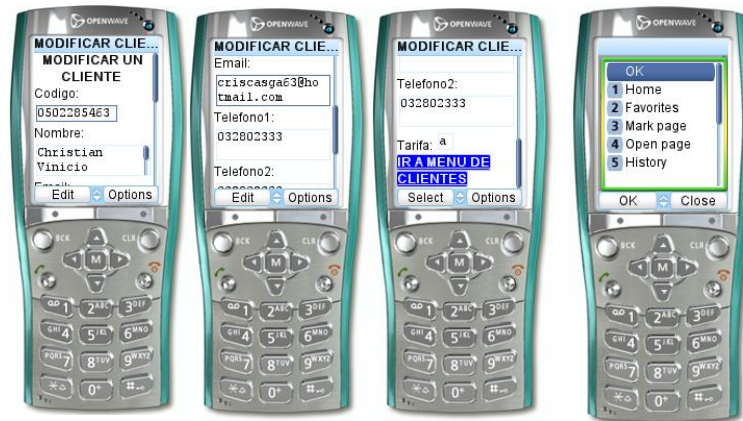
Despliega el cards buscar cliente con los campos necesarios para la búsqueda y posteriormente la modificación o eliminación.



El campo nombre cliente define el nombre del cliente que se le asigno al sujeto, el cual nos permite realizar la búsqueda de los datos correspondientes a los clientes para modificar o eliminar.

Modificación de clientes.

Despliega el cards modificar cliente con los campos necesarios para la modificación.



Presenta la información del cliente almacenado en la base de datos para su modificación.

El campo código define el código del cliente que se le asigna al sujeto, de la misma manera el nombre define el nombre completo, email el email, telefono1 y telefono2 los correspondientes números de teléfono y la tarifa la cual define el modo de nivel del cliente, esto permite controlar todo el movimiento de transacciones de dicho cliente.

Eliminación del cliente.

Al momento que se realiza la búsqueda del cliente en cards de buscar cliente se despliega la información si la búsqueda es exitosa y se procede a la eliminación seleccionando la opción de eliminar siempre y cuando no este relacionado con ningún pedido o saldo.



Si el cliente tiene pendiente algún saldo o realizo un pedido al momento de eliminar se despliega el cards mensaje de cliente.



Mostrar clientes.

Despliega el cards mostrar cliente con los datos disponibles en la base de datos para su visualización.



Administración De Artículos.

Creación de nuevos artículos.

Despliega el cards ingresar artículo con los campos necesarios para el ingreso.



El campo código define el código del artículo que se le asigna al objeto, de la misma manera el nombre define el nombre del artículo, precio_a el un precio mínimo, precio_b un precio módico, un precio_c un precio un poco elevado y el stock para saber cuantos productos consta en stock, esto permite controlar todo el movimiento de transacciones de dicho artículo.

Buscar artículo.

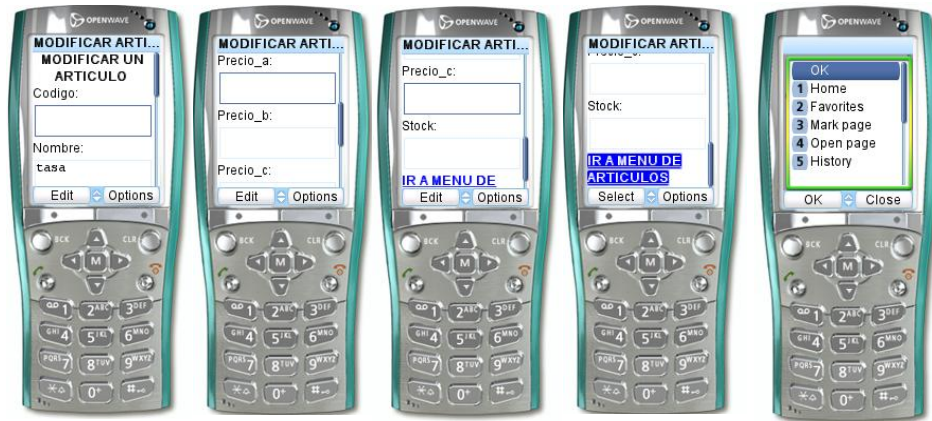
Despliega el cards buscar artículo con los campos necesarios para la búsqueda y posteriormente la modificación o eliminación.



El campo nombre artículo define el nombre del artículo que se le asigno al objeto, el cual nos permite realizar la búsqueda de los datos correspondientes a los artículos para modificar o eliminar.

Modificación de artículos.

Despliega el cards modificar artículos con los campos necesarios para la modificación.



Presenta la información del artículo almacenado en la base de datos para su modificación.

El campo código define el código del artículo que se le asigna al objeto, de la misma manera el nombre define el nombre, precio_a el un precio mínimo, precio_b un precio módico, un precio_c un precio un poco elevado y el stock para saber cuantos productos consta en stock, esto permite controlar todo el movimiento de transacciones.

Eliminación del artículo.

Al momento que se realiza la búsqueda del artículo en cards de buscar artículos se despliega la información si la búsqueda es exitosa y se procede a la eliminación seleccionando la opción de eliminar siempre y cuando no este relacionado con ningún pedido.

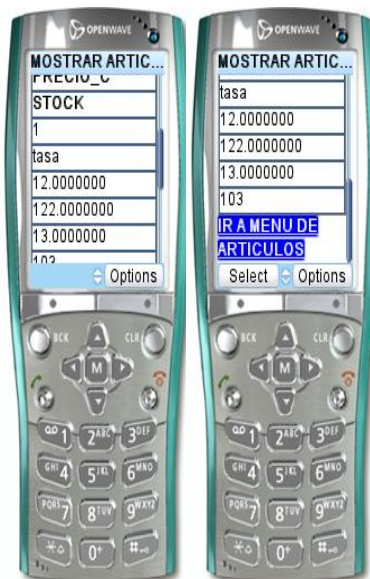


Si un artículo tiene a realizo un pedido al momento de eliminar se despliega el cards mensaje de artículo.



Mostrar artículos.

Despliega el cards mostrar artículos con los datos disponibles en la base de datos para su visualización.



Administración De Saldos.

Mostrar saldos por cliente.

Despliega el cards buscar saldos con los campos necesarios para la búsqueda.



El campo código cliente define el código del cliente que se le asigno al sujeto, el cual nos permite realizar la búsqueda de los datos correspondientes a los saldos del cliente para saber cuantos pedidos y saldos debe.

Mostrar saldos.

Despliega el cards mostrar saldos con los datos disponibles en la base de datos para su visualización.



Administración De Pedidos.

Creación de un pedido.

Despliega el cards invalides pedido con los campos necesarios para el ingreso.



El campo nombre cliente define el nombre del cliente que se le asigno al sujeto, el cual nos permite realizar la búsqueda de los datos correspondientes y validar al cliente para realizar un pedido, el cual puede ser pagado en efectivo o en cheque.

Despliega el cards pedido con lo necesario para el ingreso de un pedido.



Para añadir un artículo al pedido seleccione la opción añadir artículo el cual despliega el cards buscar artículo con los campos necesarios para el ingreso del artículo al pedido.



El campo nombre artículo define el nombre del artículo que se le asigno al objeto, el cual nos permite realizar la búsqueda del artículo si existe despliega en el mismo cards el campo de cantidad, el cual permite el ingreso del artículo al pedido, si la cantidad del artículo es mayor al stock despliega el cards de mensaje artículo con los datos correspondientes.



Para modificar un artículo seleccionamos la opción actualizar o si deseo eliminar el artículo del pedido seleccionamos la opción eliminar.

Después de los datos ingresados al pedido podemos seleccionar aceptar o cancelar, los cuales nos permite controlar si se realiza o no el pedido.

Buscar pedido

Despliega el cards buscar pedido con los campos necesarios para la búsqueda y posteriormente la modificación o eliminación.



El campo nombre código cliente define el código del cliente que se le asigno al sujeto, el cual nos permite realizar la búsqueda de los datos correspondientes del cliente y el número del pedido para modificar o eliminar.

Modificar pedido.

Despliega el cards pedido modificar con los datos necesarios para la modificación.



Para modificar un artículo seleccionamos la opción actualizar o si deseo eliminar el artículo del pedido seleccionamos la opción eliminar.

Después de los datos ingresados al pedido podemos seleccionar aceptar o cancelar, los cuales nos permite controlar si se realiza o no el pedido.

Eliminación del pedido.

Al momento que se realiza la búsqueda del cliente en cards de buscar pedido se despliega la información si la búsqueda es exitosa y se procede a la eliminación seleccionando la opción de eliminar.

6.3 Glosario de Términos.

WAP: Wireless Application Protocol o Protocolo de Aplicaciones Inalámbricas.

PDAs: Siglas para Personal Digital Assistant o Asistente Personal Digital.

http: HyperText Transfer Protocol o Protocolo de Transferencia de Hipertexto

WAE: Wireless Application Environment o Entorno de aplicación inalámbrica.

WSP: Wireless Session Protocol o Protocolo Inalámbrico de Sesión.

WTP: Wireless Transaction Protocol o Protocolo Inalámbrico de Transacciones.

WTLS: Wireless Transport Layer Security o Capa de Seguridad de Transporte Inalámbrico.

WDP: Wireless Datagram Protocol o Protocolo Inalámbrico de Datagramas.

SSL: Secure Sockets Layer.

HTML: HyperText Markup Language o Lenguaje de Marcas Hipertextuales.

XML: eXtensible Markup Language o [lenguaje de marcas](#) extensible.

WML: Wireless Markup Language.

WMLScript : Wireless markup Language Script.

WTA: Wireless Telephony Applications.

WTAI: Wireless Telephony Application Interface.

WSP: Wireless Session Protocol,

WTP: Wireless Transaction Protocol.

WWW: World Wide Web.

CID: Confidencialidad, Integridad, Disponibilidad.

SIM: Subscriber Identity Module o Módulo de Identificación del Suscriptor

PAP: Password Authentication Protocol.

CHAP: Challenge-Handshake Authentication Protocol.

ACL: Access Control Lists.

TLS: Transport Layer Security

GSM: Global System for Mobile Communications.

6.4 Bibliografía.

Libros de Consulta:

Seguridad Informática Para Empresas y Particulares (Gonzalo Álvarez Marañón y Pedro Pablo Pérez García).

Seguridad En Redes Telemáticas (Justo Carracede Gallardo).

Paginas Web:

<http://www.emagister.com/>

<http://www.wapforum.org/>

<http://www.wmlclub.com/articulos/seguridad.htm>

<http://www.wapforum.org/what/technical.htm>

<http://www.elcodigo.net/tutoriales/wap/wap2.html>

<http://www.efaber.net/proycli>

<http://geneura.ugr.es/~maribel/wap/>

<http://perso.wanadoo.es/tutoriales>

<http://www.wmlclub.com/docs/index.htm>

<http://www.apache-ssl.org/>

<http://tud.at/programm/apache-ssl-win32-howto.php3>.

http://www.chilewap.cl/cw/wap_3.html

ÍNDICE:

1	CAPÍTULO I	V
1	TECNOLOGÍA WAP Y SU FUNCIONAMIENTO	V
1.1	INTRODUCCIÓN.....	V
1.2	HISTORIA DE WAP.	V
1.2.1	Evolución Del WAP.	VI
1.2.1.1	Arquitectura WAP 1.X.....	VI
1.2.1.2	Arquitectura WAP 2.0.	IX
1.3	WIRELESS APPLICATION PROTOCOL (WAP).....	IX
1.4	COMPONENTES DE LA ARQUITECTURA WAP.....	XII
1.5	CAPA DE APLICACIÓN (WAE).....	XIII
1.5.1	Wireless Markup Language (WML).	XIII
1.5.2	Wireless markup Language Script (WMLScript).....	XIV
1.5.3	Wireless Telephony Applications (WTA).....	XIV
1.5.4	Wireless Telephony Application Interface (WTAI).	XV
1.6	CAPA DE SESIÓN (WSP).....	XV
1.7	CAPA DE TRANSACCIONES (WTP).....	XVI
1.8	CAPA DE SEGURIDAD (WTLS).	XVI
1.9	CAPA DE TRANSPORTE (WDP).....	XVII
1.10	EL ENTORNO INALÁMBRICO DE APLICACIONES.	XVII
1.11	EL PROTOCOLO INALÁMBRICO DE SESIÓN.	XIX
1.12	EL PROTOCOLO INALÁMBRICO DE TRANSACCIÓN.....	XX
1.13	EL PROTOCOLO INALÁMBRICA DE SEGURIDAD DE TRANSPORTE. XXIII	
1.14	EL PROTOCOLO INALÁMBRICO DE DATAGRAMAS.....	XXIV
2	CAPÍTULO II	XXV
2	SEGURIDADES.	XXV
2.1	INTRODUCCIÓN.....	XXVI
2.2	SEGURIDADES.	XXVI
2.2.1	Confidencialidad.....	XXVII

2.2.2	Integridad.	XXVIII
2.2.3	Disponibilidad.	XXIX
2.3	PROBLEMAS DE SEGURIDAD.	XXIX
2.3.1	Problemas De Disponibilidad.	XXIX
2.3.2	Problemas De Privacidad.	XXX
2.3.3	Problemas Técnicos.	XXX
2.3.4	Problema De Suscripción.	XXX
2.3.5	Problemas Internos.	XXXI
2.3.6	Recomendaciones Al Abonado.	XXXI
2.4	TIPOS DE SEGURIDADES Y SU FUNCIONAMIENTO.	XXXII
2.4.1	Servicios De Seguridad.	XXXII
2.4.1.1	Autenticación De La Entidad Par.	XXXII
2.4.1.2	Control De Acceso (Autorización).	XXXIV
2.4.1.3	Confidencialidad De Los Datos.	XXXV
2.4.1.4	Integridad De Los Datos.	XXXV
2.4.1.5	No Repudio.	XXXV
2.4.1.6	Clonación Y Virus.	XXXVI
2.5	LA SEGURIDAD EN WAP.	XXXVI
2.5.1	Protocolo Inalámbrico De Seguridad A Nivel De Transporte (WTLS). XXXVII	
2.5.2	Librería Criptográfica Del Lenguaje Wmlscript Crypto Library (WMLS). XXXVII	
2.5.3	Módulo De Identidad Inalámbrico (WIM).	XXXVIII
2.6	ARQUITECTURA DE SEGURIDAD WAP.	XXXVIII
2.6.1	Zona Internet: El Puente Hacia El Servidor De Aplicaciones.	XXXIX
2.6.2	Zona Inalámbrica: Del Dispositivo WAP A La Pasarela.	XL
2.6.2.1	El Medio Aéreo (GSM).	XL
2.6.2.2	Wireless Transport Layer Security (WTLS).	XLI
2.6.3	Zona Gris: La Pasarela WAP.	XLIII
2.6.4	Seguridad Extremo A Extremo.	XLIV
3	CAPÍTULO III	XLV

3	ANÁLISIS DEL MODULO DEL SISTEMA ADMINISTRATIVO INTEGRADO FENIX.	XLV
3.1	SISTEMA ADMINISTRATIVO INTEGRADO FENIX.....	XLV
3.2	ALCANCE DEL SISTEMA.....	XLVI
3.3	INFORMES.	XLVII
3.4	INFORMES ESTADÍSTICOS.	XLIX
3.5	CARACTERÍSTICAS.....	LIV
3.6	VENTAJAS.....	LIV
3.7	DESCRIPCIÓN DE LOS MÓDULOS.	LV
3.7.1	Contabilidad General.....	LV
3.7.2	Facturación.....	LVI
3.7.3	Inventarios.....	LVII
3.7.4	Caja – Bancos.....	LVIII
3.7.5	Clientes – Proveedores.	LIX
3.8	CON EL SISTEMA INTEGRADO FENIX.....	LIX
4	CAPÍTULO I V.....	LX
4	DESARROLLO DEL MODULO CARTERA DE CLIENTES (CUENTAS POR COBRAR) DEL SISTEMA ADMINISTRATIVO INTEGRADO FENIX A UN LENGUAJE WML CON PHP (APLICANDO LA METODOLOGÍA XP).....	LX
4.1	METODOLOGÍA.....	LXI
4.2	PLANIFICACIÓN.....	LXI
4.2.1	Especificación de Requisitos de Software.....	LXI
4.2.1.1	Introducción.....	LXI
4.2.1.2	Requisitos Específicos.	LXII
4.2.1.2.1	No Funcionales.....	LXII
4.2.1.2.2	Funcionales.....	LXIII
4.2.2	Usabilidad.....	LXVIII
4.3	DISEÑO.....	LXIX
4.3.1	Diseño Conceptual.	LXIX
4.3.1.1	Casos de Uso.....	LXIX
4.3.1.2	Diagrama de Secuencia.	LXXVII

4.3.1.3	Contratos de Operaciones.....	LXXXVIII
4.3.1.4	Diagrama de Clases.....	XCVI
4.3.1.5	Modelo Entidad Relación.....	XCVI
4.3.2	Diseño Navegación.	XCVIII
4.3.3	Diseño Interfaz.	CII
4.4	CODIFICACIÓN.	CVIII
4.5	IMPLEMENTACIÓN.	CIX
4.5.1	Prerrequisitos Para La Instalación.....	CIX
4.5.2	Instalación y Configuración del APACHE.....	CX
4.5.3	Creando un certificado.	CXIII
4.5.4	Instalación y Configuración del PHP.	CXVII
4.5.5	Instalación y Configuración de Mysql.	CXVII
4.5.6	Instalación del Sistema.....	CXVIII
5	CAPÍTULO V.....	CXVIII
5	CONCLUSIONES Y RECOMENDACIONES.....	CXVIII
5.1	Conclusiones.....	CXVIII
5.2	Recomendaciones.....	CXIX
6	ANEXOS.	CXX
6.1	Manual de Administrador.....	CXX
6.2	Manual de Usuario.	CXXIV
6.3	Glosario de Términos.	CXL
6.4	Bibliografía.	CXLI

ÍNDICE DE FIGURAS:

Figura 1.1:	Arquitectura Web.....	VI
Figura 1.2:	Arquitectura WAP.....	VII
Figura 1.3:	Torre de Protocolo WAP 1.x.....	VIII
Figura 1.4:	Arquitectura WAP 2.0.....	IX
Figura 1.5:	Modelo del funcionamiento del WAP.....	X
Figura 1.6:	Ejemplo de una Red WAP.....	XI
Figura1.7:	Arquitectura WAP.....	XIII

Figura 1.8: Componentes del Cliente WAE	XVIII
Figura 1.9: Ejemplo de Intercambio de Primitivas de Capa de Sesión y Transacción	XXII
Figura 1.10: Secuencia de Primitivas para el establecimiento de una sesión segura	XXIV
Figura 2.1: Principio Fundamentales De La Seguridad	XXVII
Figura 2.2: Modelo de Seguridad WAP	XXXIX
Figura 2.3: Arquitectura De Comunicaciones WAP	XLI
Figura 3.1: Módulos del Sistema Administrativo Integrado FENIX	XLVI
Figura 3.2: Gráfica De Estadísticas Por Artículo En Forma Cilíndrica.....	L
Figura 3.3: Gráfica De Estadísticas Por Ventas Total Empresa En Forma Lineal LI	
Figura 3.4: Gráfica De Estadísticas de Cartera de Clientes En Forma De Pastel LI	
Figura 3.5: Gráfica De Estadísticas Compras a Proveedores En Forma De ConosLII	
Figura 3.6: Gráfica De Estadísticas Saldos De Caja En Forma de Plano	LIII
Figura 3.7: Gráfica De Estadísticas Por Saldos De Bancos En Formato FENIXLIV	
Figura 3.8: Gráfica Del Libro Diario	LVI
Figura 3.9: Gráfica De Factura/Devolución a Clientes	LVII
Figura 3.10: Gráfica De Movimientos de Inventario	LVIII
Figura 3.11: Gráfica De Depósitos	LVIII
Figura 3.12: Gráfica De Movimientos de Cuentas Por Cobrar A Clientes	LIX
Figura 4.1: Fases De La Propuesta Metodológica XP	LXI
Figura 4.2: Requisitos no Funcionales	LXII
Figura 4.3: Requisitos para El Funcionamiento de la Aplicación.....	LXII
Figura 4.4: Requisitos Funcionales	LXIII
Figura 4.5: Requisitos Administración de Usuarios	LXIV
Figura 4.6: Requisitos Administración de Clientes	LXV
Figura 4.7: Requisitos Administración de Artículos	LXVI
Figura 4.8: Requisitos Administración de Pedidos	LXVII
Figura 4.9: Requisitos Administración de Saldos	LXVIII
Figura 4.10: Casos de Uso.....	LXX
Figura 4.11: Actores	LXX

Figura 4.12: Casos de Uso Administración de Usuarios	LXXI
Figura 4.13: Casos de Uso Administración Clientes	LXXII
Figura 4.14: Casos de Uso Administración Artículos	LXXIII
Figura 4.15: Caso de Uso Administración Pedidos	LXXV
Figura 4.16: Casos de Uso Administración de Saldos	LXXVI
Figura 4.17: Diagrama de Secuencia Control de Usuario	LXXVII
Figura 4.18: Diagrama de Secuencia Añadir Usuario	LXXVIII
Figura 4.19 Diagrama de Secuencia Modificar Usuario	LXXIX
Figura 4.20: Diagrama de Secuencia Eliminar Usuario	LXXIX
Figura 4.21: Diagrama de Secuencia Añadir Cliente.....	LXXX
Figura 4.22: Diagrama de Secuencia Modificar Cliente	LXXX
Figura 4.23: Diagrama de Secuencia Eliminar Cliente	LXXXI
Figura 4.24: Diagrama de Secuencia Reporte Cliente	LXXXI
Figura 4.25: Diagrama de Secuencia Añadir Artículo.....	LXXXII
Figura 4.27: Diagrama de Secuencia Modificar Artículo	LXXXII
Figura 4.28: Diagrama de Secuencia Eliminar Artículo	LXXXIII
Figura 4.29: Diagrama de Secuencia Reporte Artículos	LXXXIII
Figura 4.30: Diagrama de Secuencia Añadir Pedido.....	LXXXV
Figura 4.31: Diagrama de Secuencia Modificar Pedido	LXXXVI
Figura 4.32: Diagrama de Secuencia Eliminar Pedido	LXXXVII
Figura 4.33: Diagrama de Secuencia Reporte Saldos por Cliente	LXXXVII
Figura 4.33: Diagrama de Secuencia Reporte Saldos	LXXXVIII
Figura 4.34: Diagrama de Clases del Sistema WAP	XCVI
Figura 4.35: Vista Lógica del modelo Entidad Relación	XCVII
Figura 4.36: Vista Física del Modelo Entidad Relación	XCVIII
Figura 4.37: Interfaz de Manejo de Administración De Usuario	XCIX
Figura 4.38: Interfaz de Manejo deL Ingreso y Menú Principal del Sistema.....	XCIX
Figura 4.39: Interfaz de Manejo de Administración De Clientes.....	C
Figura 4.40: Interfaz de Manejo de Administración De Usuario	C
Figura 4.41: Interfaz de Manejo de Administración De Usuario	CI
Figura 4.42: Interfaz de Manejo de Administración De Usuario	CI

Figura 4.43: Ingresando Al Sistema. Emulador WAP	CII
Figura 4.44: Menús Del Sistema. Emulador WAP	CII
Figura 4.45: Registro De Clientes. Emulador WAP	CIII
Figura 4.46: Búsqueda y Validación Del Cliente. Emulador WAP	CIII
Figura 4.47: Modificación y Validación Del Cliente. Emulador WAP	CIII
Figura 4.48: Reporte De Los Clientes. Emulador WAP	CIV
Figura 4.49: Registro De Artículos. Emulador WAP	CIV
Figura 4.50: Búsqueda y Validación De Artículos. Emulador WAP	CV
Figura 4.51: Modificación y Validación De Artículos. Emulador WAP	CV
Figura 4.52: Reporte De Los Artículos. Emulador WAP	CVI
Figura 4.52: Validación Del Ingreso Del Pedido. Emulador WAP	CVI
Figura 4.53: Validación Del Pedido. Emulador WAP	CVI
Figura 4.54: Búsqueda y Validación Del Pedido. Emulador WAP	CVII
Figura 4.55: Modificación y Validación Del Pedido. Emulador WAP	CVII
Figura 4.55: Reporte De Los Saldos Por Un Cliente. Emulador WAP	CVII
Figura 4.56: Reporte De Los Saldos Por Un Cliente. Emulador WAP	CVIII
Figura 4.57: Archivo de configuración del servidor Apache	CX
Figura 4.58: Pantalla De Creación de Certificado	CXIV
Figura 4.59: Remueve Contraseña en Creación de un Certificado	CXV
Figura 4.60: Expedición de Tiempo de un Certificado	CXVI
Figura 4.61: Certificado Creado	CXVII

ÍNDICE DE TABLAS:

Tabla 2.1: Clases De La Implementación De Seguridad WTLS	XLIII
--	-------