UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas

"SISTEMA DE MEDIOS DE PAGOS USANDO TELEFONIA MOVIL"

Informe de Suficiencia

Para optar el titulo Profesional de:

INGENIERO DE SISTEMAS

Alexander Emilio Tong Vicente

Lima-Perú

2006

DEDICATORIA

A mí adorada esposa Karina, por su apoyo incondicional.

AGRADECIMIENTOS

Mi sincero agradecimiento a mi padres por el apoyo brindado, por enseñarme a no rendirme y hacer realidad mis sueños.

A mi esposa Karina que siempre estuvo a mi lado apoyándome en los momentos más difíciles.

A mi amigo Cristian Fuentes quien me permitió ser parte del proyecto MovilCash.

A Telefónica, por iniciarme en la línea consultaría de Call Center e IVR, y por brindarme las oportunidades necesarias para poder desarrollar mis habilidades en un ambiente de ética profesional, gracias Miriam Vilitanga.

INDICE

		Pag.
DESCRIPTORES TEMATICOS		1
RESUMEN		2
INTRODUCCION		4
CAPITULO I		
ANTECEDENTES		6
1.1	Diagnóstico Estratégico	6
1.1.1	Fortalezas y Debilidades	6
1.1.2	Oportunidades y Riesgos	6
1.2	Diagnostico Funcional	7
1.2.1	Productos	7
1.2.2	Clientes	9
1.2.3	Proveedores	9
1.2.4	Procesos	10
1.2.5	Organización de la Empresa	10
CAPITULO II		
MARCO TEORICO		14
2.1	Introducción a la Telefonía	14
2.2	Computador y Teléfono	17
2.2.1	Integracion Computador Teléfono (CTI)	18
2.2.2	Tarjetas de Voz	19
2.3	IVR (Interactive Voice Response)	20

2.3.1 Arquitectura IVR 20
2.4 CT ADE 21
2.5 WAP (Wireless Application Protocol) 23
2.5.1 Arquitectura WAP 24
2.6 SSL (Secure Socket Layer) 24
2.6.1 Protocolos Secure Socket Layer 29
2.6.2 Implementación del Protocolo SSL 34
CAPITULO III
PROCESO DE TOMA DE DECISIONES 36
3.1 Planteamiento del Problema 36
3.2 Alternativas de Solución 37
3.3 Metodología de la Solución 45
3.4 Toma de Decisiones 47
3.5 Estrategias Adoptadas 47
CAPITULO IV
EVALUACION DE RESULTADOS 60
CAPITULO V 63
CONCLUSIONES
CAPITULO VI 64
RECOMENDACIONES
GLOSARIO DE TERMINOS 65
BIBLIOGRAFIA 66
ANEXOS 67
ANEXO 1 67
ANEXO 2 74
ANEXO 3 76
ANEXO 4 80

DESCRIPTORES TEMÁTICOS

- TELEFONIA MOVIL.
- SISTEMA IVR.
- WAP.
- SSL.
- PROTOCOLOS SSL.
- INTEGRACION COMPUTADOR TELEFONO.
- TARJETAS DE TELEFONIA.
- TELEFONIA IP.
- SISTEMA DE MEDIOS DE PAGOS.
- METODOLOGIA PMI.

RESUMEN

Telefónica Empresas es una empresa creada por el Grupo Telefónica para optimizar el servicio de soluciones de comunicación y tecnologías de la información del sector empresarial peruano, con un catálogo de productos y servicios que puedan satisfacer de manera integral sus necesidades.

Telefónica Empresas nace con el respaldo de la experiencia adquirida en Telefónica Data (que integró Telefónica Sistemas, Telefónica Servicios Financieros, Telefónica Servicios Internet) y la Gerencia Central de Comunicaciones de Empresas.

Telefónica Empresas no sólo atiende a las grandes corporaciones del país, sino también a las grandes y medianas empresas. Es la ventanilla única de atención de todos los servicios para el segmento empresarial.

Ofrece servicios a la medida de las necesidades de los clientes, con tecnología avanzada y mayor cobertura. Esto le permite ser proveedora integral de soluciones de comunicación y servicios de información para mejorar la eficacia en la gestión de las compañías; entre los clientes mas importantes que confían en la calidad de servicio de Telefónica Empresas son: VISA Perú y Banco de Crédito.

Uno de los servicios que ofrece Telefónica Empresas es la infraestructura de medios de pagos transaccionales POS de VISA Perú. En la actualidad los comercios que desean acceder a este servicio de medio de pago POS deben realizar la solicitud a VISA Perú, para lo cual los comercios deben cumplir una serie de requisitos como: monto de mínimo de venta mensual, capital de la empresa. Finalmente una vez que VISA Perú aprueba la solicitud del Comercio, VISA Perú solicita a Telefónica Empresas que

suministre el equipamiento y la infraestructura de comunicaciones al comercio.

Debido al costo de equipamiento y la infraestructura de comunicaciones, se planteo una solución de que permita lo siguiente:

- Contar con un medio de pagos que no involucre costos altos en equipamiento e infraestructura de comunicaciones y reemplace el POS actual.
- Contar con toda la seguridad a nivel transaccional que ofrece un POS actual.
- Sea fácil de usar.

Para ello se analizo las tecnologías que actualmente dispone Telefónica Empresas y se decidió usar la tecnología que ofrece la Telefonía Móvil, teniendo en cuenta que es un medio mas accesible y económico para los comercios.

Este reto me permitió aplicar la experiencia que tengo en telefonía (IVR) además de incorporar el uso de otras tecnologías como Transaccional, WAP y WEB en la elaboración del nuevo producto.

INTRODUCCION

El presente informe de suficiencia tiene como objetivo principal demostrar como la implementación del sistema de pagos usando Telefonía Móvil que desarrolle en Telefónica Empresas, logro un impacto positivo tanto en la empresa proveedora de medios de pagos como VISA y Telefónica Empresas, así como en el comercio.

El enfoque de la solución conlleva a la creación de una nueva plataforma de medios de pagos, nunca antes usada, haciendo uso de la tecnología Transaccional, WAP, IVR, WEB.

La concepción del nuevo sistema trae en si una solución que sea amigable para los comercios, fácil de usar, portable, económica, que cuenten con la información actualizada y toda la seguridad transaccional.

Esta solución plantea la implementación de los siguientes servicios:

- Un servicio web, mediante el cual tanto los compradores y vendedores se podrán afiliar al sistema (previa aprobación), además de poder consultar sus operaciones realizadas.
- Un servicio WAP, desde el cual los vendedores podrán realizar las transacciones con los medios de pagos tarjeta de crédito y/o debito, el cual estará conectado directamente al Banco, contando con toda la seguridad electrónica para realizar una transacción segura.

- Un servicio IVR, desde el cual el cliente confirmara la transacción realizada por el vendedor.

Resumiendo la solución planteada nos brindara los siguientes beneficios:

- Soluciones para la realización de ventas de los comercios distribuidores utilizando tarjetas de crédito / débito o cargos en cuenta bancaria de una manera sencilla y segura.
- Soluciones que permitan desplazar el uso de los POS tradicionales por cuestiones de costos: mantenimiento e instalación de la red, gastos generales (papel, cableado, HW / SW y reprogramaciones), viabilidad técnica, entre otros.

La gestión del proyecto siguió rigurosamente la metodología PMI, gracias a la cual se mantuvo un control de todas las actividades y los riesgos que se presentaban. Mi participación se dio durante todo el proceso del proyecto, esto me permitió tener una concepción del proyecto a nivel tecnológico y de gestión.

CAPITULO I
ANTECEDENTES

1.1 Diagnóstico Estratégico

1.1.1 Fortalezas y Debilidades

Fortalezas

- T-Empresas es una empresa con un solidó respaldo económico.
- T-Empresas cuenta con cobertura nacional en la comunicación.
- El sistema esta focalizado en un segmento de mercado de grandes empresas.

Debilidades

- T-Empresas tiene poca sectorización del mercado.
- T-Empresas es una organización con demasiados procedimientos, para la entrega de productos y servicios.
- T-Empresas es una organización ligada a muchas políticas españolas, la cual no le permite explorar el mercado peruano.
- El catalogo de servicios y productos que provee T-Empresas aun es muy costoso para el sector mediano y Pymes.

1.1.2 Oportunidades y Riesgos

Oportunidades

- Mercado cautivo para seguir explotándolo.
- Recurso Humano calificado para contratar.

- Renovación constante de nuevos servicios y productos para el mercado.
- Ser la empresa líder en soluciones de telecomunicaciones.

Riesgos

- Nuevas Empresas de telecomunicaciones como Telmex, Millicon, IMSA, entre otras.
- Empresas que brindan soluciones de ingeniería como GMD, IBM, Cosapi, Telmex, HP, Adexus, Electrodata entre otras
- El control de calidad de productos estándar no muy especifico en T-Empresas.

1.2 Diagnostico Funcional

1.2.1 Productos

Telefónica Empresas ofrece los siguientes productos:

Datos: Soluciones en la comunicación de datos, ofreciendo los siguientes servicios:

- **Redes Privadas Virtuales Local y Nacional:** Soluciones orientadas a la formación de VPNs que integra oficinas dispersas geográficamente permitiendo compartir entre ellas aplicaciones de voz, datos y video con alta calidad y disponibilidad.
- **Transporte Internacional:** Servicios que interconecta distintos lugares del mundo permitiendo transmitir a través de fibra óptica o satélite, información basada en la conmutación de datos, es un servicio de conexión de redes que utiliza como medio de transporte la red IP MPLS internacional de Telefónica Empresas.

Internet: Servicios de conectividad a Internet, ofreciendo los siguientes servicios:

- **Conexión:** Soluciones para la conexión a Internet utilizando diferentes medios de acceso: terrestres y satelitales, de acuerdo a los requerimientos específicos de las empresas.
- **Soluciones:** Servicio de valor añadido que complementa al servicio InfoInternet Empresarial, incorporando cuatro módulos de seguridad,

perimetral y de contenidos, con los cuales se protege la información contenida en la red del cliente.

Data Center: Administración del servicio con niveles especializados, ofreciendo los siguientes servicios:

- **Soluciones Web y Content Delivery:** Familia de servicios de Infraestructura de espacio físico, IT, Comunicaciones y Operación con altas prestaciones para cualquier aplicación o desarrollo en el entorno Internet.
- **Hosting y Servicios gestionados:** La familia de Hosting y servicios gestionados cubre las necesidades de infraestructura de alta disponibilidad, provisión de plataformas, monitoreo y administración que requieren las aplicaciones de misión crítica de las empresas de la era e-business.
- **Servicios Aplicaciones y Help Desk:** Servicio integral basado en las tecnologías de información con objetivos y necesidades específicas que permite gestionar a través de un único punto de contacto toda la infraestructura IT de un cliente, permitiendo eficiencias en sus procesos y ahorros en sus costos.

E-Solutions: Consultoría, diseño e integración a medida Internet, ofreciendo los siguientes servicios:

- **Ingeniería de Redes:** Soluciones tecnológicas de infraestructura de redes para el transporte, procesamiento, almacenamiento y acceso a la información.
- **Seguridad:** Soluciones integrales basados en estándares que aseguran la confidencialidad, integridad y disponibilidad de los activos de información y de las transacciones minimizando los riesgos.
- **Software de Negocios:** Soluciones de negocio y aplicativos que permiten mejorar los procesos de una empresa y las relaciones con sus clientes. Para ello se cuenta con soluciones E- Business, atención al cliente, soluciones móviles y transaccionales.

Voz: Comunicación y transmisión de voz a nivel nacional, ofreciendo los siguientes servicios:

- **Línea Troncal:** Servicio que permite dar acceso a una comunicación local, nacional e internacional; por medio de una línea telefónica fija. Permite a las empresas una mejor administración de llamadas.
- **Red Digital de Servicios Integrados:** Servicio de telefonía digital que permite con un único acceso, comunicaciones simultáneas de voz, datos y video con alta fiabilidad y calidad de transmisión.
- **Centrales Telefónicas PBX:** Provee una gama completa de equipos de comunicaciones que satisfacen las necesidades de empresas pequeñas, medianas y grandes empresas.

1.2.2 Clientes

Telefónica Empresas no sólo atiende a las grandes corporaciones del país, sino también a los grandes grupos empresariales, PYMEs y SOHOs, y es además la ventanilla única de atención de todos los servicios para el segmento empresarial, los cuales podemos mencionar:

- Clientes del Sector Gobierno.
- Clientes del Sector Educativo.
- Clientes del Sector Minero.
- Clientes del Sector Bancario y Financiero.
- Clientes del Sector Seguros.
- Clientes del Sector Salud.
- Pymes

1.2.3 Proveedores

Telefónica Empresas para poder brindar una calidad de servicio cuenta con proveedores nacionales e internacionales, los cuales podemos mencionar:

- Proveedores de Equipos de Redes.
- Proveedores para Equipamiento de Data Centers.
- Proveedores para Equipamiento de Equipos de Seguridad Informática.
- Proveedores de Soluciones de Telefonía IP.
- Proveedores de Soluciones de Software.

1.2.4 Procesos

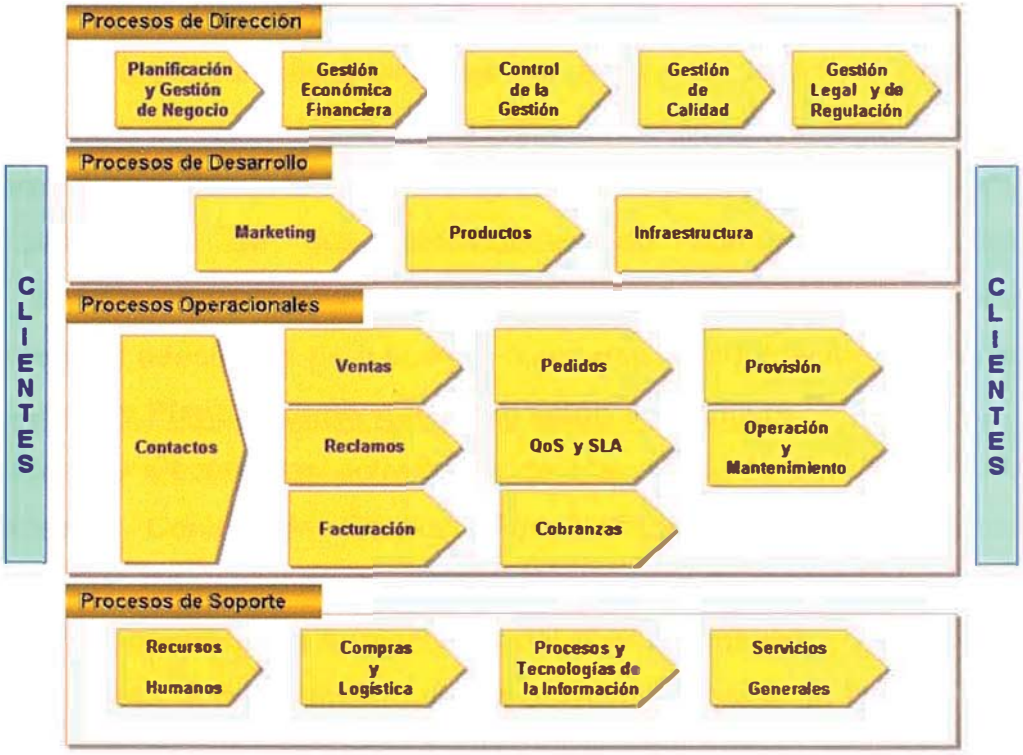


Fig. 1

1.2.5 Organización de la Empresa

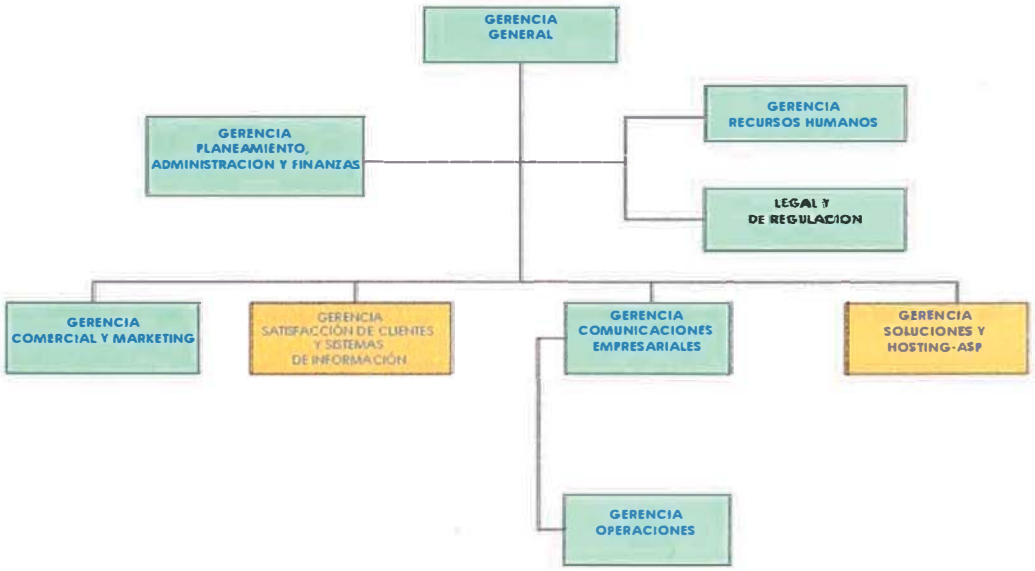


Fig. 2

a. Gerencia General

Formular y determinar la política y el plan estratégico de la empresa dentro de las facultades otorgadas por el Comité Directivo, coordinado y controlando las actividades de los diferentes servicios funcionales de la misma, desarrollando la eficiencia operativa de nuestros clientes a través de la satisfacción de sus necesidades de comunicación avanzadas brindándoles un nivel optimo de calidad, permitiendo así obtener niveles de rentabilidad adecuados para nuestra compañía y para nuestros accionistas.

b. Gerencia Planeamiento Administración y Finanzas

Liderar y ejecutar las actividades de Planeamiento Estratégico, Análisis Financiero, Control de Gestión, Administración, Compras, Facturación, Cobranzas, Contabilidad, Tesorería, Gestión de Contratas, asegurando la evaluación oportuna de la ejecución del plan estratégico y coordinando las acciones para el cumplimiento de los objetivos y metas de la empresa y del grupo.

c. Gerencia Recursos Humanos

Optimizar la administración de Recursos Humanos a través de la gestión por competencias dirigiendo el potencial de los empleados hacia el desarrollo personal y profesional, elevando el nivel de compromiso e identificación en el desempeño de sus funciones y fortaleciendo una cultura organizacional en la cual las personas, sus capacidades y competencias y valores sea nuestra mayor ventaja competitiva.

d. Gerencia Legal y Regulación

Velar por el cumplimiento de los derechos y obligaciones de la empresa adquiridos mediante los contratos de concesión y por las normas dispuestas por los organismos reguladores del estado Peruano: OPSITEL (Organismo Supervisor de Inversión Privada de Telecomunicaciones) y MTC (Ministerio de Transporte y Comunicaciones).

Asimismo brindar asesoria legal a todas las áreas de la empresa en lo concerniente a las actividades legales, referidas a asuntos civiles,

corporativos, tributarios, administrativos, entre otros< con el fin de asegurar la corrección de estos actos en la empresa.

e. Gerencia Comercial y Marketing

Efectuar el control de seguimiento del desarrollo de las líneas de negocio, gestión de ventas y de la calidad de atención al cliente, así mismo, coordinar las gestiones de comunicación, prensa y difusión de la identidad corporativa, a fin de cumplir los objetivos anuales del negocio.

f. Gerencia Satisfacción al Cliente y Sistemas de Información

Asegurar y fortalecer el compromiso con los clientes a largo plazo, a través de sus unidades organizativas en coordinación con las áreas de la empresa, proveedores, cambios tecnológicos y tendencias de los mercados.

h. Gerencia Comunicaciones Empresariales

Diseño, desarrollo e implantación de soluciones integrales en telecomunicaciones, basadas en productos y servicios de Conectividad: Voz, Datos, Internet, así como el control de calidad de redes y servicios; asegurando la actualización e incremento del valor de los productos y servicios ofrecidos, así como la satisfacción de los clientes y el fortalecimiento de las relaciones como socios estratégicos.

i. Gerencia Soluciones y Hosting-ASP

Diseño, desarrollo e implantación de soluciones integrales en telecomunicaciones, basadas en productos y servicios E-Solutions: Ingeniería de Redes, Seguridad y E-Business. Gestionar todos los productos de Infraestructura del Data Center (Housing, Hosting, CPI Virtual, Distribución de Contenido, Multimedia, Disaster Recovery), los servicios de soporte y mantenimiento de soluciones; en coordinación con las diversas áreas de la empresa, proveedores, cambios tecnológicos y tendencias de los mercados; asegurando la actualización e incremento de valor de los productos y servicios ofrecidos así como la satisfacción de los clientes y el fortalecimiento de las relaciones como socios estratégicos.

Además, complementa las soluciones con productos y servicios de socios y/o Alianzas estratégicas.

j. Gerencia Operaciones

Planificar y ejecutar la provisión de servicios, al gestión de recursos de red, el mantenimiento de redes, la asistencia técnica y mantenimiento de servicios o EDC en clientes, el soporte en las operaciones, a fin de asegurar los estandares de calidad de operadores de redes y servicios.

CAPITULO II
MARCO TEORICO

2.1 Introducción a la Telefonía

Existen diversas definiciones sobre la telefonía, para tener mas clara esta palabra previamente definiremos algunos conceptos.

Comunicación, significa compartir información en forma escrita, por voz, no verbales (ejemplo el Lenguaje de cuerpo) o electrónica (ejemplo las telecomunicaciones).

Sistemas de comunicaciones, son sistemas electrónicos que transmiten información a través de líneas de un lugar a otro

Comunicación electrónica, es la comunicación que se establece con personas u organizaciones que pueden estar a grandes distancias haciendo uso de las computadoras y de redes electrónicas.

Conectividad, significa que un usuario pueda conectarse a una microcomputadora mediante un teléfono usando otros vínculos se conectan a otras computadoras y fuentes de información desde casi cualquier lugar geográfico del mundo. Mediante esta conexión, el usuario se encuentra en vinculo con otras computadoras en el globo terráqueo. Los tipos de computadoras pueden ser minicomputadores y macrocomputadores ("maninframe"). Las opciones para la conectividad incluyen:

- Maquinas de fax.
- Boletines electrónicos.
- Correo electrónico.
- Recursos compartidos.
- Servicios en línea.

Telecomunicaciones, este es un concepto más complejo y amplio. Las telecomunicaciones representa la transmisión, recepción y conmutación de información (ejemplo datos, televisión, fotos, audio y facsímiles entre otros) a través de distancias empleando señales eléctricas u ópticas (que se expresa en forma oral, telégrafo, la radio, teléfono o por señales de computadoras), enviadas mediante alambre o medio electromagnético (ejemplo a través del aire).

El proceso de comunicación sigue un patrón particular: una fuente de información envía información a través de un canal de información (medio), para alcanzar un receptor de información.

Estos conceptos lo podemos encontrar en un diccionario o en el Diccionario de electrónica e Informática: Bod Edgard (Ejecutivo de Dialogic una de las empresas que proveen hardware y software de comunicaciones) define la telefonía como una parte del mundo de las telecomunicaciones, que involucra a todos los equipos y la comunicación entre ellos, y que permite que un usuario se puede comunicar ya sea con un teléfono de casa o celular con otro usuario. Este concepto es compartido por la gran mayoría de autores de los textos de electrónica.

Para que dos teléfonos se puedan comunicar existe en la PSTN (la Red Publica de Telefonía). La PSTN es muy similar a una red WAN de transmisión de datos la única diferencia es que es una red que se va a encargar de transmitir voz, mediante el uso de la línea análoga para poder conectarse a esta red.

El teléfono se ha convertido en estos últimos tiempos en uno de los tantos medios de comunicación mas usados. Incluso debido a sus costos y fácil accesibilidad empresas locales, lo utilizan para poder comunicarse con sus clientes, proveedores, socios, etc.; sin embargo debido a que las necesidades comunicación de las empresas son muy diferentes a la que ofrece un teléfono convencional (teléfono de casa), se requieren de equipos mas sofisticados de comunicación llamados PBX, y que permiten atender varias llamadas en forma simultanea, contar con mas opciones de telefonía como: transferencia de llamada, conferencia de llamada, colocar una

llamada en espera, etc., y de poder conectar varios teléfonos que permita atender todas llamadas que reciben desde la PSTN. Las PBXs cuentan con softwares que facilitan la configuración y administración; y pueden ser instalados desde una PC contando estos con interfaces de consola, visuales, y web.

Muchas de las PBXs cuentan con arquitectura bastante robusta, por lo que en la actualidad la mayoría de empresas todavía lo utiliza a pesar de las bondades que la Tecnología de Voz por IP entrega.

Así mismo, existen otros tipos de líneas telefónicas, además de la línea análoga y la fibra óptica para la PBX, que permiten conectarme a la PSTN. Estas líneas son de tipo digital y entregan características adicionales, además de permitir la conexión a la PSTN, hacen uso de un servidor y una tarjeta de voz realizan un trabajo similar a una PBX (mas adelante detallaremos al respecto).

T1 : También conocido como DS1 (Digital Service level 1), T1 es una troncal digital que contiene 24 canales o líneas, que trabaja bajo diversos tipos de protocolos de comunicación como ISDN, CAS, Q.SIG, etc.; e incluye características avanzadas, como el numero ANI y DNIS. Este tipo de línea se utiliza para transmisión de datos, y para transmisión de voz. Es usado en Norte América o USA y Japón.

E1 : Usado fuera de Norte América, como Europa y Latinoamérica, es el tipo de troncal digital más común, este entrega 30 canales o líneas. Maneja protocolos de comunicación tales como Euro-ISDN, E1-CAS, etc., e incluye características avanzadas al igual que el T1 como reconocimiento de ANI y DNIS. También es usado para transmisión de datos y entregan un tamaño grande ancho de banda en redes WAN.

T3 : Llamado también DS3 es el siguiente paso sobre E1 o T1. Este tipo de linea entrega 576 canales o líneas, lo cual es equivalente a 24 T1s o 18 E1s en una simple troncal digital.

BRI ISDN : Conocido también como BRI o Basic Rate Interface, entrega 2 canales o líneas en una troncal simple, y es usado también por los usuarios de casa. Presenta características similares al T1 o E1 como el ANI y DNIS,

se utiliza también para datos y como linea de contingencia cuando existe una linea E1 o T1 para comunicaciones de voz.

Conforme crecen las necesidades de comunicación tanto de datos como de voz, estas redes se hacen más complejas, debido a ello nace la Voz por IP y la Telefonía IP, como una mejor forma de poder comunicarse y además de poder usar en una misma red la voz y los datos y para tener una mejor administración de los recursos de ellos. Así como existe el protocolo TCP/IP para datos, la Telefonía IP y Voz por IP usa de los protocolos H.323 y SIP (Session Initiation Protocol); el SIP es un protocolo nuevo de comunicación, mientras que el protocolo mas usado es el H.323. La Tecnología Voz por IP permite transmitir paquetes de voz por la red de datos y la Tecnologia de Telefonía IP hace que estos paquetes de datos transmitidos por la red puedan llegar a un dispositivo llamado Teléfono IP conectado a la red de datos la voz ofreciendo las mismas características que ofrece un teléfono convencional (análogo).

Debido a que la voz realmente consume 64 Kbps por segundo existen algoritmos de compresión que permite mejorar considerablemente este ancho de banda, lográndose así ahorrar costos en ancho de banda de la red y proporcionándole una mejor fluidez a los paquetes de datos, algo que no sucede con Internet. Entre estos algoritmos tenemos el G.723.1, G711 y G729, con distintas tasas de compresión cada uno. La tasa también lo define los fabricantes de equipos que se encargan de administrar las llamadas de Voz por IP o Telefonía IP (algo similar a la PBX). Los equipos IP manejan datos y no voz como lo hacen las PBX normalmente, por lo cual hacen uso de un equipo llamando Gateway, el que permite conectarse al mundo de voz y convertirlo a datos, posteriormente estos equipos vuelven a convertir el dato a voz y son transmitidos a equipos teléfonos mas conocidos como Teléfonos IP.

2.2 Computador y Teléfono

Actualmente la tecnología en computadores se ha desarrollado muy rápidamente, tanto en capacidad para poder almacenar información como en

velocidad de procesamiento de información. La telefonía también ha avanzando de igual manera ya que actualmente un administrador desde una PC puede llevar toda la administración de una central telefónica. La integración ha llegado a tal punto en el que podemos ver programas de computadoras desde donde puede administrar un teléfono, es decir poder realizar llamadas, colgar, transferencia, conferencia, etc. en forma rápida y sencilla, permitiendo además poder integrarse a los sistemas corporativos y/o aplicativos que pueden existir en una empresa. A continuación detallaremos algunos conceptos que nos permitirá entender mejor esta tecnología.

2.2.1 Integracion Computador Teléfono (CTI)

Integración computador teléfono también conocido como CTI o Solución CTI, es la integración vía software entre el computador y la PBX, en la cual un computador puede recibir información de la central telefónica acerca de eventos telefónicos tales como llamadas entrantes, llamadas colgadas, transferidas, etc.; y también ofrecer funciones de control de llamadas vía APIs y comandos de consola a través del computador desde donde se puede realizar funciones como colgar llamadas, contestar llamadas, retener llamadas, transferir llamadas, etc. Entre las funcionalidades que describimos podremos resaltar la transferencia de llamada: una solución CTI que además de realizar la transferencia telefónica de forma convencional, agrega una funcionalidad muy especial: la transferencia de llamada; asociada con información.

Estas funcionalidades pueden ser aprovechadas por los sistemas corporativos y aplicativos que hacen uso de la tecnología CTI, dando un gran valor agregado a la atención al cliente en los Call Center.

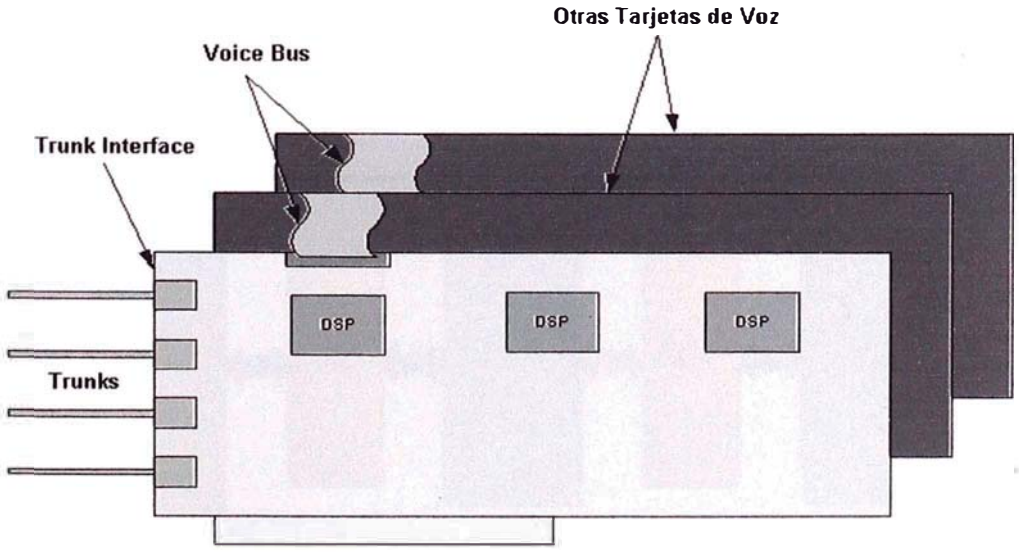
Para lograr la integración CTI el computador y la PBX se conecta mediante un enlace denominado CTI link, que puede ser una línea serial R2-232, Ethernet u otro tipo de conexión a la red.

2.2.2 Tarjetas de Voz

Las tarjetas de voz son dispositivos encargados del procesamiento de voz, cuentan con microprocesadores DSP, encargados de procesar señales digitalizadas de audio en forma eficiente; ofreciendo: una alta calidad de audio, conexión simultanea a un gran numero de líneas telefónicas y algoritmos para el análisis de progreso de llamada, compresión y descompresión de audio (para una mejor manejo de los paquetes de voz), y cancelación de eco entre otras características.

Las tarjetas son insertadas o agregadas en el computador soportando diversos tipos de buses (ISA, PCI) y conectándose varios tipos de líneas (análogas, E1, T1, T3, BRI). Las distintas líneas pueden trabajar juntas, es decir es posible conectar 2 o más tarjetas de tal forma que se pueda administrar mayor cantidad de líneas, desarrollándose una trabajo similar a la de una pequeña PBX.

Otras características importante es que las tarjetas de voz están aptas para soportar las nuevas tecnologías de voz: TTS (conversión texto a voz) y ASR (reconocimiento de voz). En el mercado podemos encontrar tarjetas de fabricantes como Aculab y Dialogic, que se rigen bajo ciertos estándares comunes, pero también podemos encontrar otras tarjetas propietarias.



Tarjeta de Voz

Fig. 3

Trunks : Medio o puerta de conexión de la tarjeta a las líneas telefónicas

Trunks Interface : Contenedor de Trunks de la Tarjeta

Voice Bus : Cable para la conexión con otras tarjetas

2.3 IVR (Interactive Voice Response)

Interactive Voice Response es también conocido como IVR aunque existen muchos autores que lo definen como VRU, sin embargo, el nombre más comercial y más conocido es IVR. Son sistemas encargados de contestar llamadas y atender al usuario llamante vía mensajes pregrabados. Adicionalmente, algunos sistemas IVR están conectados a sistemas corporativos que responden a peticiones en las que se requiere de extraer información de tales sistemas.

Los IVRs han permitido automatizar muchas tareas que los Call Center realizan, para ello hacen uso de las tarjetas de voz y de softwares. Es justamente, mediante softwares, que se realiza la programación de los IVRs, ello ha permitido que puedan conectarse a diversos tipos de sistemas corporativos, además de poder hacer uso de la tecnología de voz como TTS y ASR.

Una solución IVR es instalada en un computador, comúnmente llamado servidor IVR, el cual contiene además las tarjetas de voz.

2.3.1 Arquitectura IVR

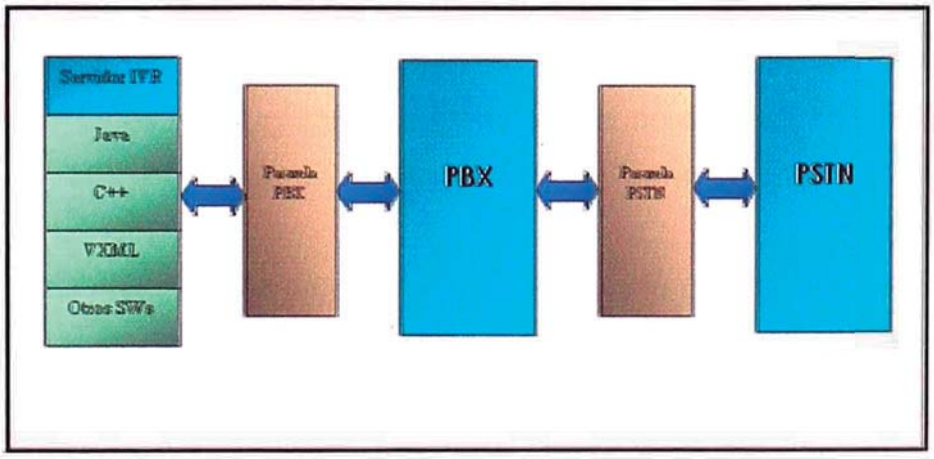


Fig. 4

Servidor IVR: Encargado de realizar el tratamiento de la llamada, en algunos casos interactúa con una Base de Datos y otros repositorios de información; el IVR puede ser desarrollado en lenguajes de programación como Java, C++, VXML, entre otros.

Pasarela PBX: Puede ser un medio físico (Tarjeta de Telefonia) o lógico el cual permite conectarse al servidor IVR, esta pasarela permite trasmitir las instrucciones a la central como: contestar llamada, transferir llamada, colgar, etc.

PBX: Mas conocido como central telefónica que se encarga de recibir las llamadas de la Red Publica de Telefonía.

Pasarla PSTN: Medio físico (E1, BRI, T1, etc.) encargado de conectar la Central Telefónica con la Red Publica de Telefonía, los cuales pueden ser análogo o digital dependiendo de la arquitectura de la central telefónica.

PSTN: Red Pública de Telefonía encargada de canalizar todas las llamadas provenientes de los teléfonos instalados en oficinas, casas, celulares, etc.

2.4 CT ADE

CT ADE es un lenguaje para el desarrollo de aplicaciones IVR y CTI de la familia de productos de Intel. CT ADE lenguaje de fácil aprendizaje que provee un runtime engine muy compacto y de alta performance el cual soporta las tecnologías de procesamiento de voz mas populares.

CT ADE es compatible, a nivel de fuente y binario, bajo los siguientes sistemas operativos: Windows 95, Windows NT, SCO-UNIX y DOS. Esta característica única le permite portar las aplicaciones VOS sobre cualquier sistema operativo protegiendo su inversión de desarrollo. VOS incluye un lenguaje muy completo y detallado, que le permite crear todo tipo de aplicaciones CTI.

CT ADE es mas sencillo pero a la vez mas robusto de "C/C++" así mismo es mucho más poderoso que los simples "lenguajes de codificación" (scripting languages). Por ejemplo, VOS soporta expresiones aritméticas y lógicas con uso de paréntesis, operadores "y", "o", "no", funciones y subrutinas con

parámetros nombrados (named parameters) y variables privadas, bibliotecas de funciones con códigos reutilizables y muchas otras características.

CT ADE es compatible con un rango mucho mas amplio de opciones de hardware y de software que ninguna otra herramienta. VOS cuenta con una garantía de funcionamiento para cualquier combinación de placas Dialogic soportando mas de 100 protocolos internacionales de señalización y múltiples APIs.

CT ADE puede leer directamente, escribir y compartir bases de datos con otras aplicaciones en distintos formatos tipo: dBase III, dBase IV, Clipper, FoxPro, Jet y ADO incluyendo servidores SQL, ODBC, Paradox, Btrieve, Excel, Lotus y otros.

CT ADE le permite construir casi cualquier aplicación CTI para el procesamiento de llamadas de manera mucho más rápida y sencillo que lenguajes de programación tipo C/C++ y con mucha mayor flexibilidad que la mayoría de los "generadores de aplicaciones".

De esta manera, una solución con CT ADE permitirá las siguientes funcionalidades:

- Reconocimiento de tonos DTMF: Permite el reconocimiento DTMF con una eficiencia del 100 %.
- Interrupción de Eco: Esta tecnología permite que el usuario interrumpa la locución dando la información que el sistema le está solicitando sin necesidad de esperar a que finalice el mensaje de interrogación.
- Grabación de Mensajes: El sistema es capaz de grabar y reproducir mensajes en forma digital, cuenta además con una herramienta que permite crear, editar y organizar los archivos de voz y grabar locuciones con acento peruano.
- Tiempo de Respuesta: El tiempo de respuesta del sistema IVR (una vez qué la llamada ingresa al sistema) es inmediato.
- Diagrama de Flujo: Permite la creación y ejecución de múltiples menús, así como la modificación e incorporación de nuevas rutinas.
- Generación de Reportes: El sistema almacena información sobre:

Hora en qué se inició la llamada.

Duración de la llamada.

Número de llamadas rechazadas.

Número de llamadas según el motivo de la finalización.

Número de llamadas finalizadas exitosamente y transferida a operadora.

Cantidad total de llamadas atendidas por cada puerto.

Cantidad total de llamadas atendidas por el sistema.

- Conexión ODBC: El sistema IVR Vox permite la conexión nativa o vía ODBC a Base de Datos relacionales.
- Conexión PBX: El sistema se conecta a la PBX por medio de líneas telefónicas analógicas (anexos analógicos) o a través de E1-Line Side.
- Conexión a la RTB: El sistema se conecta a la RTB por medio de líneas telefónicas analógicas (troncales analógicos), o a través de interfaces digitales tales E1, T1, ISDN, R2, etc.

2.5 WAP (Wireless Application Protocol)

WAP es el acrónimo de *Wireless Application Protocol*, que podríamos traducir como Protocolo de Aplicación Inalámbrico. La tecnología WAP es realmente un estándar impulsado por la industria del sector de las telecomunicaciones con el objetivo de proporcionar un sistema avanzado de servicios de internet para dispositivos móviles.

La tecnología tiene como premisas iniciales el uso de estándares abiertos ya existentes (como los protocolos HTTP, o el XML), la independencia de la tecnología de comunicaciones móviles sobre la que se implemente (en principio, GSM, pero en el futuro podría ser GPRS o incluso UMTS) y la independencia del terminal móvil (desde un teléfono hasta un PDA).

A partir de las premisas anteriores, el conjunto de protocolos incluidos en el estándar WAP debe adaptarse a las condiciones propias de un entorno totalmente nuevo, como es el de las comunicaciones móviles. En concreto, la red de comunicaciones presenta limitaciones de ancho de banda

importantes, alta latencia y cobertura intermitente, y los terminales de acceso no tienen grandes capacidades de procesamiento, ni de memoria, además de utilizar pantallas que no permiten más de 4 o 5 líneas de texto.

Todas estas particularidades se han tenido en cuenta a la hora de diseñar los protocolos y la arquitectura del sistema WAP.

2.5.1 Arquitectura WAP

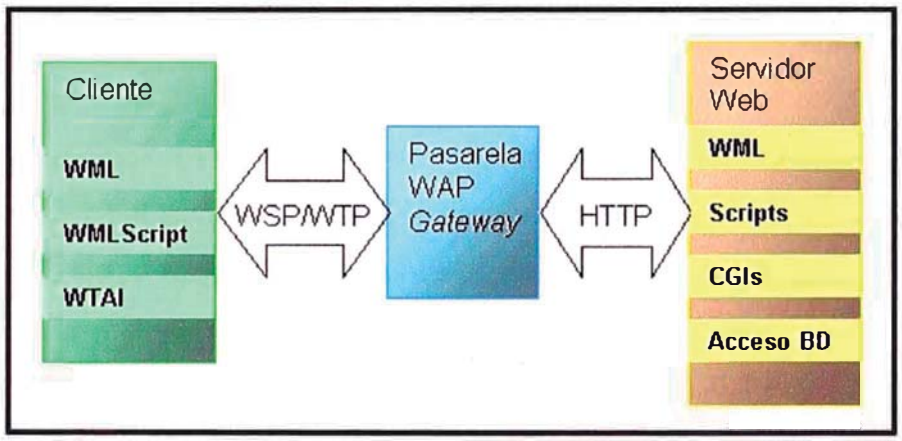


Fig. 5

El cliente o dispositivo WAP está provisto de un micro-navegador que constituye la interfaz de usuario para realizar las funciones de navegación. El micro-navegador interpreta páginas WML. El WML sería el equivalente al HTML del Internet "fijo".

La pasarela realiza 2 funciones básicas: conversión de protocolos (de HTTP a WSP/WTP y viceversa) y codificación / decodificación de las páginas WML. Estos procesos permiten la adaptación a la red inalámbrica del protocolo y de los contenidos.

Finalmente, en el servidor web residen las páginas, así como cualquier otra lógica basada en CGIs, acceso a bases de datos o lenguajes de script. WAP es compatible con servidores HTTP 1.1, lo que facilita la adopción del estándar por parte de los proveedores de contenidos web ya existentes.

2.6 SSL (Secure Socket Layer)

En la actualidad, para garantizar que una transacción sea segura por la red se debe contemplar los aspectos de Autenticidad, Integridad,

Confidencialidad y No Repudio. Son varios los sistemas y tecnologías que se han desarrollado para intentar implementar estos aspectos en las transacciones electrónicas, siendo sin duda SSL (Secure Socket Layer) es más conocido y usado en la actualidad. SSL permite la Confidencialidad y la Autenticación en las transacciones por Internet, siendo usado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. SSL es una de las formas base para la implementación de soluciones PKI (Infraestructura de Clave Publica).

SSL (Secure Socket Layer) es un sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communications Corporation, y está basado en la aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet, como consecuencia puede resultar difícil para un atacante o Hacker Informático poder obtener o manipular información que pasa por este canal seguro. De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación, mientras que los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la Confidencialidad en la transmisión de datos.

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket (nombre de máquina más puerto), de forma transparente al usuario y a las aplicaciones que lo usan.

Actualmente es el estándar de comunicación segura en los navegadores web más importantes (protocolo HTTP), como Nestcape Navigator e Internet Explorer, y se espera que pronto se saquen versiones para otras otros protocolos de la capa de Aplicación (correo, FTP, etc.).

La identidad del servidor web seguro (y a veces también del usuario cliente) se consigue mediante el Certificado Digital correspondiente, del que se comprueba su validez antes de iniciar el intercambio de datos sensibles (Autenticación), mientras que de la seguridad de Integridad de los datos

intercambiados se encarga la Firma Digital mediante funciones hash y la comprobación de resúmenes de todos los datos enviados y recibidos.

Desde el punto de vista de su implementación en los modelos de referencia OSI y TCP/IP, SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de Aplicación y la capa de Transporte, sustituyendo los sockets del sistema operativo, lo que hace que sea independiente de la aplicación que lo utilice, y se implementa generalmente en el puerto 443. (NOTA: Los puertos son las interfaces que hay entre las aplicaciones y la pila de protocolos TCP/IP del sistema operativo).

Fig.6

SSL proporciona servicios de seguridad a la pila de protocolos, encriptando los datos salientes de la capa de Aplicación antes de que estos sean segmentados en la capa de Transporte y encapsulados y enviados por las capas inferiores. Es más, también puede aplicar algoritmos de compresión a los datos a enviar y fragmentar los bloques de tamaño mayor a 214 bytes, reensamblándolos nuevamente en el receptor.

La versión más actual de SSL es la 3.0. que usa los algoritmos simétricos de encriptación DES, TRIPLE DES, RC2, RC4 e IDEA, el asimétrico RSA, la función hash MD5 y el algoritmo de firma SHA-1. Los algoritmos, longitudes de clave y funciones hash de resumen usados en SSL dependen del nivel de seguridad que se busque o se permita, siendo los más habituales los siguientes:

- **RSA + Triple DES de 168 bits + SHA-1:** Soportado por las versiones 2.0 y 3.0 de SSL, es uno de los conjuntos más fuertes en cuanto a seguridad, ya que son posibles $3.7 * 10^{50}$ claves simétricas diferentes, por lo qu e

muy difícil de romper. Por ahora sólo está permitido su uso en Estados Unidos, aplicándose sobre todo en transacciones bancarias.

- **RSA + RC4 de 128 bits + MD5:** Soportado por las versiones 2.0 y 3.0 de SSL, permite $3.4 * 10^{38}$ claves simétricas diferentes que, aunque es un número inferior que el del caso anterior, da la misma fortaleza al sistema. Análogamente, en teoría sólo se permite su uso comercial en Estados Unidos, aunque actualmente ya es posible su implementación en los navegadores más comunes, siendo usado por organismos gubernamentales, grandes empresas y entidades bancarias.
- **RSA + RC2 de 128 bits + MD5:** Soportado sólo por SSL 2.0, permite $3.4 * 10^{38}$ claves simétricas diferentes, y es de fortaleza similar a los anteriores, aunque es más lento a la hora de operar. Sólo se permite su uso comercial en Estados Unidos, aunque actualmente ya es posible su implementación en los navegadores más comunes.
- **RSA + DES de 56 bits + SHA-1:** Soportado por las versiones 2.0 y 3.0 de SSL, aunque es el caso de la versión 2.0 se suele usar MD5 en vez de SHA-1. Es un sistema menos seguro que los anteriores, permitiendo $7.2 * 10^{16}$ claves simétricas diferentes, y es el que suelen traer por defecto los navegadores web en la actualidad (en realidad son 48 bits para clave y 8 para comprobación de errores).
- **RSA + RC4 de 40 bits + MD5:** Soportado por las versiones 2.0 y 3.0 de SSL, ha sido el sistema más común permitido para exportaciones fuera de Estados Unidos. Permite aproximadamente $1.1 * 10^{12}$ claves simétricas diferentes, y una velocidad de proceso muy elevada, aunque su seguridad es ya cuestionable con las técnicas de Criptoanálisis actuales.
- **RSA + RC2 de 40 bits + MD5:** En todo análogo al sistema anterior, aunque de velocidad de proceso bastante inferior.
- **Sólo MD5:** Usado solamente para autentificar mensajes y descubrir ataques a la integridad de los mismos. Se usa cuando el navegador cliente y el servidor no tienen ningún sistema SSL común, lo que hace imposible el establecimiento de una comunicación cifrada. No es soportado por SSL 2.0, pero si por la versión 3.0.

La clave de encriptación simétrica es única y diferente para cada sesión, por lo que si la comunicación falla y se debe establecer una nueva sesión SSL, la contraseña simétrica se generará de nuevo.

SSL proporciona cifrado de alto nivel de los datos intercambiados (se cifran incluso las cabeceras HTTP), autenticación del servidor (y si es necesario también del cliente) e integridad de los datos recibidos.

Durante el proceso de comunicación segura SSL existen dos estados fundamentales, el **estado de sesión** y el **estado de conexión**. A cada sesión se le asigna un número identificador arbitrario, elegido por el servidor, un método de compresión de datos, una serie de algoritmos de encriptación y funciones hash, una clave secreta maestra de 48 bytes y un flag de nuevas conexiones, que indica si desde la sesión actual se pueden establecer nuevas conexiones. Cada conexión incluye un número secreto para el cliente y otro para el servidor, usados para calcular los MAC de sus mensajes, una clave secreta de encriptación particular para el cliente y otra para el servidor, unos vectores iniciales en el caso de cifrado de datos en bloque y unos números de secuencia asociados a cada mensaje.

¿Cómo podemos saber si una conexión se está realizando mediante SSL?. Generalmente los navegadores disponen de un icono que lo indica, generalmente es un candado en la parte inferior de la ventana. Si el candado está abierto se trata de una conexión normal, y si está cerrado de una conexión segura. Si hacemos doble click sobre el candado cerrado nos aparecerá el Certificado Digital del servidor web seguro.

Fig. 7

Además, las paginas que proceden de un servidor SSL vienen implementadas mediante protocolo HTTP seguro (HTTPS), por lo que su

dirección, que veremos en la barra de direcciones del navegador, empezará siempre por https, como por ejemplo:
https://www.htmlweb.net
Por último, cuando estamos en una conexión segura podemos ver el certificado del servidor acudiendo al menú "Archivo" del navegador y haciendo click en el botón de "Propiedades". En la parte inferior tenemos una opción "Certificados", que nos mostrará el del servidor actual.

2.6.1 Protocolos Secure Socket Layer

Para establecer una comunicación SSL es necesario que previamente el cliente y el servidor realicen un proceso de reconocimiento mutuo y de petición de conexión que, al igual que en otros tipos de comunicaciones, recibe el Handshake, que en este caso está controlado por el **Protocolo SSL Handshake**, que se encarga de establecer, mantener y finalizar las conexiones SSL. Durante ese momento se negocian los parámetros generales de la sesión y los parámetros particulares de cada conexión.
Concretamente, y de forma general, el protocolo comienza con el saludo del cliente al servidor, conocido como **Client Hello**, por el que se informa al servidor del cual se desea establecer una comunicación segura con él. SSL soporta solicitudes de conexión por puertos diferentes al utilizado normalmente para este servicio. Junto con este saludo inicial, el cliente envía al servidor información de la versión de SSL que tiene implementada, de los algoritmos de encriptación que soporta, las longitudes de clave máximas que admite para cada uno de ellos y las funciones hash que puede utilizar. También se le solicita al servidor el envío de su Certificado Digital X.509 v3, con objeto de verificar el cliente la identidad del mismo y recoger su clave pública. En este momento se asigna un identificador a la sesión y se hace constar la hora y fecha de la misma.
Como medida adicional, el cliente envía asimismo una clave numérica aleatoria, para que se pueda establecer una comunicación segura mediante otros protocolos o algoritmos en el caso de que el servidor web no posea un Certificado Digital.

En este paso no se intercambia en ningún momento información sensible, tan sólo información necesaria para establecer la comunicación segura.

A continuación, el servidor SSL responde al cliente en el proceso que se conoce con el nombre de **Server Hello**, enviándole su Certificado Digital (con su llave pública) e informándole de su versión de SSL, de los algoritmos y longitudes de clave que soporta.

Generalmente se obtiene el conjunto de algoritmos, longitudes de clave y funciones hash soportados por ambos, eligiéndose entonces los más fuertes. Si no hay acuerdo con los algoritmos a usar se envía un mensaje de error.

A veces, y si la comunicación posterior así lo exige, el servidor solicita al cliente su Certificado Digital, en el mensaje llamado **CertificateRequest**. Esto sólo suele ocurrir en SSL cuando los datos a transferir sean especialmente sensibles y precisen la previa autenticación del cliente. Si es el caso, el cliente debe contestar al servidor mediante el mensaje **CertificateVerify**, enviándole entonces su certificado.

En este momento el cliente verifica la validez del Certificado Digital del servidor, desencriptando el resumen del mismo y comprobando su corrección, verificando que ha sido emitido por una Autoridad Certificadora de confianza, que esté correctamente firmado por ella y que el certificado no esté revocado. También se comprueba que la fecha actual está dentro del rango de fechas válidas para el certificado y que el dominio (URL) que aparece en el certificado se corresponde con el que se está intentando establecer la comunicación segura. Si alguna de estas validaciones falla, el navegador cliente rechazará la comunicación, dándola por finalizada e informando al usuario del motivo del rechazo.

En caso de que el servidor no tenga un Certificado X.509 v3 se puede utilizar un mensaje **ServerKeyExchange** para enviar la clave pública sin certificado, en cuyo caso queda en manos del cliente la elección de si acepta la llave o no, lo que finalizaría el proceso.

Como medida adicional de seguridad, el cliente genera una clave aleatoria temporal y se la envía al servidor, que debe devolvérsela cifrada con su clave privada. El cliente la descifra con la llave pública y comprueba la

coincidencia, con lo que está totalmente seguro de que el servidor es quién dice ser. Y un proceso análogo a éste, pero en sentido inverso, se requiere si es necesaria la autenticación del usuario ante el servidor.

Si todo está correcto el cliente genera un número aleatorio que va a servir para calcular una clave de sesión correspondiente al algoritmo de encriptación simétrico negociado antes, conocida con el nombre de **clave maestra**, que es enviada al servidor de forma segura encriptándola asimétricamente con la llave pública del mismo que aparece en el Certificado Digital. Esta clave maestra se usará para generar todas las claves y números secretos utilizados en SSL.

Con esto servidor y cliente se han identificado y tienen en su poder todos los componentes necesarios para empezar a transmitir información cifrada simétricamente.

Se pasa entonces el control al subprotocolo Change Cipher Spec, iniciándose la conexión segura.

Así y todo, para que empiecen las transmisiones de datos protegidos se requiere otra verificación previa, denominada **Finished**, consistente en que cliente y servidor se envían uno al otro una copia de todas las transacciones llevadas a cabo hasta el momento, encriptándola con la llave simétrica común. Al recibir esta copia, cada host la desencripta y la compara con el registro propio de las transacciones. Si las transacciones de los dos host coinciden significa que los datos enviados y recibidos durante todo el proceso no han sido modificados por un tercero. Se termina entonces la fase Handshake.

Para empezar a transmitir datos cifrados en necesario que cliente y servidor se pongan de acuerdo respecto a la forma común de encapsular los datos que se van a intercambiar, es decir, qué formato de datos se va a usar en la transmisión cifrada. Esto se realiza mediante el **Protocolo SSL Record** (Protocolo de Registro SSL), que establece tres componentes para la porción de datos del protocolo:

1. MAC-DATA: código de autenticación del mensaje.
2. ACTUAL-DATA: datos de aplicación a transmitir.

3. PADDING-DATA: datos requeridos para rellenar el mensaje cuando se usa un sistema de cifrado en bloque.

El Protocolo de Registro es el encargado de la seguridad en el intercambio los datos que le llegan desde las aplicaciones superiores, usando para ello los parámetros de encriptación y resumen negociados previamente mediante el protocolo SSL Handshake. Sus principales objetivos son:

Fig. 8

- La fragmentación de los mensajes mayores de 214 bytes en bloques más pequeños.
- La compresión de los bloques obtenidos mediante el algoritmo de compresión negociado anteriormente.
- La autenticación y la integridad de los datos recibidos mediante el resumen de cada mensaje recibido concatenado con un número de secuencia y un número secreto establecidos en el estado de conexión. El resultado de esta concatenación se denomina **MAC**, y se añade al mensaje. Con esta base, la autenticación se comprueba mediante el número secreto, compartido por el cliente y el servidor, y mediante el número de secuencia, que viaja siempre encriptado. La integridad se comprueba mediante la función hash negociada.

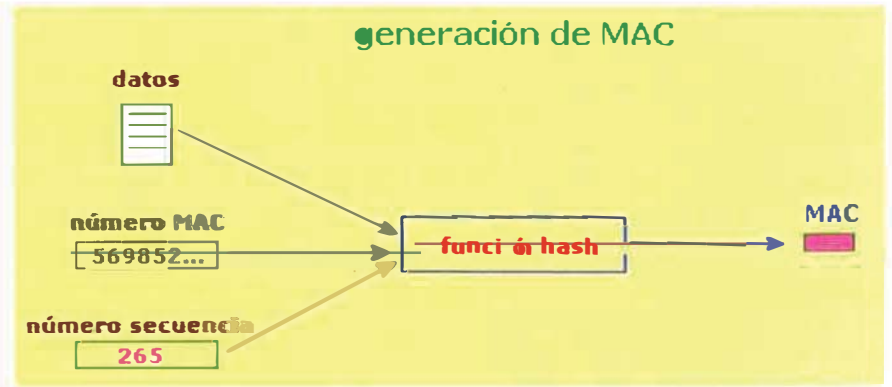


Fig. 9

- La confidencialidad se asegura encriptando los bloques y sus resúmenes mediante el algoritmo simétrico y la clave correspondiente negociadas en la fase Handshake. Existen dos tipos posibles de encriptación:

a. **Cifrado en bloque**: se cifran los datos en bloques de 64 bits. Si el mensaje no es múltiplo de 64 bits se le añaden los bits de relleno necesarios para obtener un número entero de bloques completos, indicándose la adición en el formato del mensaje. Este método de cifrado se conoce con el nombre de **Cipher Block Chainning, CBC**, y precisa un vector inicial, que habrá sido negociado previamente en la fase Handshake. Como algoritmos de cifrado se usan RC2 y DES.
b. **Cifrado Stream:** o de flujo, en el que se encriptan los datos realizando una operación lógica OR-Exclusiva entre los bytes y un generador pseudoaleatorio usando el algoritmo RC4.

Tras todos estos requisitos, el canal seguro está listo para empezar la transmisión de datos de forma segura. Cuando el cliente o el servidor desean transmitir algún mensaje al otro se genera automáticamente un resumen del mismo mediante la función has acordada, se encriptan mensaje y resumen con la clave simétrica acordada y se envían los datos. Cuando el destinatario los recibe, desencripta todo, vuelve a obtener el resumen a partir del original y lo compara con el recibido. Si coinciden hay seguridad de que la comunicación segura se ha producido satisfactoriamente, sin intromisiones externas. Si no coinciden, se pone en conocimiento del otro host, y si es preciso se suspende la conexión SSL. Cada uno de los mensajes enviados por cliente o servidor sufre este proceso de verificación.

Por último, cuando la transferencia de mensajes ha finalizado y se desea cerrar la comunicación segura, generalmente porque el cliente así lo desea, la aplicación cliente (por ejemplo el navegador web) lanza una ventana de aviso de que se va a cerrar la comunicación SSL, y si es aceptada por el usuario, se sale de la misma y se regresa a una comunicación normal, finalizando el proceso SSL.

SSL actúa computacionalmente como una máquina de estados: durante el intercambio de datos hay en todo momento un estado de escritura activo y

otro pendiente y lo mismo ocurre respecto a la lectura de datos, realizándose el cambio de estados mediante un subprotocolo especial del Handshake denominado **Change Cipher Spec**.

SSL Handshake posee además otro subprotocolo específico, denominado **Alerta**, que se encarga de avisar de los problemas que ocurren durante la conexión, y que pueden llevar a la finalización brusca de la sesión.

2.6.2 Implementación del Protocolo SSL

Por la parte del cliente, SSL viene implementado por defecto en los navegadores Internet Explorer y Nestcape Navigator, lo que permite a cualquier usuario con uno de estos navegadores poder realizar compras por Internet de forma segura sin tener que conocer el sistema a fondo ni preocuparse de instalar programas adicionales (por lo menos autenticando al servidor web y con confidencialidad e integridad asegurada en la transacción).

La implementación en la parte servidora (la tienda o banco por lo general) es un poco más compleja. En primer lugar, es obligatoria la obtención de un Certificado Digital para el vendedor o para el servidor seguro, solicitándolo a una Autoridad Certificadora de prestigio reconocido, conviniendo, si es posible, que dicha autoridad sea Verisign, ya que la misma está considerada como de toda confianza por los navegadores cliente, por lo que viene activada por defecto en los navegadores cliente; en actualidad existe otros proveedores tales como Thawte, InstantSSL, Entrust, Baltimore y Geotrust.

Ya con el servidor certificado, el usuario podrá realizar su compra. En el momento del pago, el vendedor obtiene el PIN de la tarjeta de crédito del cliente, la fecha de caducidad y sus datos personales (si el pago se realiza por este método), por lo que deberá disponer de algún sistema que permita el envío de estos datos a una entidad financiera capaz de realizar la transferencia bancaria necesaria para completar el pago.

Existen en el mundo diferentes entidades bancarias y financieras que ofrecen estos sistemas a los comerciantes, realizándose la comunicación entre comerciante y banco a través de un protocolo seguro privado en la mayoría de los casos, de forma similar a lo que ocurre cuando pagamos en

una tienda "real" con nuestra tarjeta de crédito. Estos sistemas se suelen conocer con el nombre genérico de **Pasarelas de Pago**.

Un sistema de pasarela más avanzado es el denominado **TPV**, **Terminal de Punto de Venta**. En el mismo se conecta una terminal especial al servidor web del vendedor, y mediante un software basado en script CGI se realiza la comunicación segura entre ellos.

Existen en la actualidad diferentes versiones del conjunto de protocolos SSL que se pueden implementar en los distintos servidores y que corren bajo los sistemas operativos más comunes (IIS en Windows NT-2000-XP, Apache en Unix, etc.).

CAPITULO III
PROCESO DE TOMA DE DECISIONES

3.1 Planteamiento del Problema

Telefónica Empresas ofrece soluciones de Tecnología de Información y Comunicaciones. Dentro de su cartera de soluciones están las soluciones transaccionales: soluciones que involucran los medios de pagos con tarjeta de crédito VISA.

Las soluciones transaccionales ofrecidas por Telefónica Empresas son las siguientes:

- Implementación de equipos POS en establecimientos Comerciales.
- Implementación de Paginas Web (Carritos de Compras), haciendo uso de la tarjeta de crédito como medio de pago.

Estas soluciones trabajan bajo un modelo de negocio en el cual el comprador inicia el proceso de compras y ejecuta los siguientes pasos:

- El comprador se acerca al establecimiento o negocio.
- El comprador elige los productos a comprar.
- Una vez que el comprador decide los productos a adquirir, entrega al vendedor el medio de pago (tarjeta de crédito).
- El vendedor, mediante un equipo POS, ingresa los datos de la compra como el monto y la moneda

- Si el sistema POS responde con éxito, el proceso de compra finaliza.

Adicionalmente, existe otro modelo de negocio en el cual es el vendedor quien inicia el proceso de compra, y se rige por el siguiente procedimiento:

- El vendedor se apersona al comprador.
- El vendedor ofrece sus productos al comprador.
- Una vez qué el comprador decide qué productos adquirir, el vendedor registra la información manualmente o en un equipo móvil (PALM).
- La información registrada por el vendedor es enviada en línea o al finalizar el día a un Sistema de Información.
- Finalmente el vendedor envía el comprobante de pago al comprador, para que el comprador realice el pago respectivo. El pago se realiza de acuerdo al compromiso establecido entre el comprador y vendedor.

El modelo de negocio en el cual el vendedor inicia el proceso de compras es usado por empresas que prefieren ofrecer productos a compradores potenciales.

La Gerencia de Soluciones y Hosting ASP de Telefónica Empresas ha encontrado en este modelo una oportunidad de negocio. Sin embargo, Telefónica Empresas no cuenta con un sistema que soporte este modelo de negocio y que permita cerrar la operación de compra mediante la realización del pago de manera electrónica haciendo uso de los medios de pagos como tarjeta de crédito. Las ventajas de la presente propuesta es minimizar costos operativos al vendedor y agilizar el proceso de compras.

3.2 Alternativas de Solución

Para brindar una solución a este problema, se formo un equipo de trabajo en la Gerencia de Soluciones y Hosting ASP y en el que participe como Ingeniero de Software.

Se busco alternativas que permitan a los clientes (vendedores/negociantes) trabajar en el modelo de negocio en el cual el vendedor inicia el proceso de

compras. El objetivo fue brindar una solución que permita minimizar costos operativos y agilizar el proceso.

Para diseñar la solución consideramos que el producto final debería tener las siguientes características:

- Un Sistema de Medio de Pago que no involucre costos altos en equipamiento e infraestructura de comunicaciones.
- Un Sistema con Seguridad Transaccional, similar a la que ofrece un equipo POS.
- Un Sistema que sea fácil de usar.

Como alternativas de solución analizamos las siguientes:

Alternativa 1: Sistema de Medios de Pagos usando Tecnología IVR.

En esta alternativa el comprador y el vendedor usan la tecnología IVR mediante un dispositivo móvil (celular), bajo el siguiente procedimiento:

- El vendedor realiza una llamada al número del sistema de medios de pagos mediante un dispositivo móvil (celular).
- El sistema proporciona un menú vocal que guía al vendedor en el uso del mismo:
  - Ingreso de usuario y contraseña.
  - Ingreso de los datos de la transacción.
- Cuando el vendedor finaliza el ingreso de los datos de la transacción, el sistema realiza una llamada al comprador.
- El comprador escucha mediante mensajes vocales los datos de la operación.
- Si el comprador esta de acuerdo con la transacción, confirma la operación ingresando su número de PIN.
- Finalmente, el sistema realiza una llamada al vendedor indicando que el comprador acepto la operación.

Ventajas

- Se cubren las funcionalidades requeridas.
- Se usa la herramienta de software (CT ADE) para lograr la integración a sistemas transaccionales, y Tarjetas de Telefonía Digitales **Dialogic** con la finalidad de obtener el número telefónico del usuario llamante.
- La solución garantiza un nivel de aceptación rápido.
- La solución garantiza una transacción segura y con un tiempo de respuesta no menor de 5 seg.
- La solución implementa protocolo SSL de manera que garantiza la seguridad en las transacciones realizadas.
- La solución garantiza la seguridad en la transmisión de los datos mediante la implementación de una red IP-VPN (VISA y Red de Móviles).
- Se hace uso de la Tecnología IVR, para guiar al comprador y al vendedor con mensajes de voz en el proceso de compras
- Se hace uso de dispositivo móviles digitales (no se requiere de equipos con tecnología WAP).
- La solución esta implementada bajo una sola tecnología, la de IVR.
- Telefónica Empresas cuenta con la experiencia en el desarrollo de soluciones IVR.
- La actualización de la tecnología del sistema esta garantizada por al empresa proveedora del software.
- La implementación y el mantenimiento del Sistema estaría a cargo de Telefónica Empresas.
- La solución puede migrar a un sistema, en el cual tanto el comprador y/o vendedor realizan las operaciones vía comandos de voz (reconocimiento de voz).

Desventajas

- El Sistema ofrece al vendedor un menú de voz que puede resultar largo y engorroso.
- Se requiere demasiados puertos de IVR (Tarjetas de Voz), ya sea para realizar llamadas entrantes y salientes, lo cual encarece la solución.
- La actualización de la solución requiere inversión tanto en software como en hardware.
- Se requiere mayor validación de información ante duplicidad de data.
- Se requiere dos plataformas: una de desarrollo y otra de producción con las mismas características ante cualquier actualización o cambio en el Sistema.
- Se requiere de grabaciones de audio en estudio ante cualquier cambio en el menú de voz para el comprador.

Alternativa 2: Sistema de Medios de Pagos usando Tecnología WAP

En esta solución el comprador y vendedor hacen uso de la tecnología WAP mediante un dispositivo móvil (celular). Esta alternativa trabaja de la siguiente manera:

El vendedor se conecta al sistema de medios de pagos mediante la opción WAP de su dispositivo móvil (el vendedor se autentica al sistema ingresando su usuario y password).autentica

El vendedor ingresara los datos de la operación en el dispositivo móvil.

Finalizado el ingresar de datos de la operación, el comprador ingresa a la opción de operaciones pendientes del sistema de medios de pagos y busca la operación que registró el vendedor.

Una vez que el comprador se encuentre conforme con la operación, procederá a aceptar dicha operación ingresando su numero de PIN.

- Culminada la aceptación de la operación, el vendedor desde su dispositivo móvil verificara cuales fueron las operaciones autorizadas por los compradores.
- El vendedor ingresara los datos de la operación en el dispositivo móvil.
- Finalizando el ingresar de datos de la operación, el comprador ingresa a la opción de operaciones pendientes del sistema de medios de pagos y busca la operación que registró el vendedor.
- Una vez que el comprador se encuentre conforme con la operación, procederá a aceptar dicha operación ingresando su numero de PIN.
- Culminada la aceptación de la operación, el vendedor desde su dispositivo móvil verificara cuales fueron las operaciones autorizadas por los compradores.

Ventajas

- Se cubren todas las funcionalidades requeridas en el Sistema.
- Se hace uso de un servidor Web **Internet Information Server de Microsoft** y la aplicación cuenta con la arquitectura de componentes COM, siendo esta una plataforma estable en otras soluciones WEB y WAP ya implementadas (por lo cual se ha desestimado alternativas como Apache, Personal Web Server, WebSphere, etc.).
- Se usa la Tecnología WAP, con menús y opciones para las operaciones del comprador y vendedor.
- La solución garantiza una transacción segura y con un tiempo de respuesta no menor de 5 seg.
- La solución implementa protocolo SSL de manera qué garantiza la seguridad en las transacciones realizadas.
- Se garantiza la seguridad en la transmisión de los datos mediante el uso de una red IP-VPN (VISA y Red de Móviles).
- La solución esta implementada bajo una sola tecnología que

es WAP.

- La solución puede migrar a un sistema, en el cual tanto el comprador y/o vendedor realizan las operaciones vía comandos de voz (reconocimiento de voz).
- Telefónica Empresas cuenta con al experiencia en el desarrollo de soluciones WAP.
- La actualización de la tecnología del sistema esta garantizada por al empresa proveedora del software.
- La implementación del Sistema estaría a cargo de Telefónica Empresas.

Desventajas

- El Sistema cuenta con demasiadas opciones y pasos para autorizar una operación.
- No se cuenta con muchas implementaciones a nivel local.
- Se requiere una mayor validación de información ante duplicidad de data.
- Se requiere capacitar al personal de Telefónica Móviles para el soporte Post-Implementación.
- Se requiere instalar más servidores en la plataforma WAP actual.
- Se requiere una plataforma de desarrollo y producción de las mismas características ante cualquier actualización o cambio en el Sistema.

Alternativa 3: Sistema de Medios de Pagos usando Tecnología Móvil (IVR, WEB y WAP).

En esta solución el comprador hace uso de la tecnología IVR, y el vendedor hace uso de la Tecnología WAP, ambos utilizan dispositivos móviles (celular).Esta alternativa trabaja de la siguiente manera:

- El vendedor se conecta desde su dispositivo móvil al sistema de medios de pagos, mediante la opción WAP de su dispositivo móvil (el vendedor se deberá autenticar al sistema ingresando su usuario y password).
- El vendedor ingresa los datos de la operación en el dispositivo móvil.
- Al finalizar el ingreso de los datos de la operación, el sistema de medios de pagos realiza una llamada al comprador.
- El sistema de medios de pagos indica al comprador desde el dispositivo móvil, los datos de la operación.
- Así mismo, solicita la confirmación de la operación, si el comprador esta de acuerdo ingresa el numero de PIN.
- Luego de que el comprador autoriza la operación, el sistema de medios de pagos envía un mensaje SMS al celular indicando que la operación fue aceptada.

Ventajas

- Se cubren todas las funcionalidades que son requeridas en el Sistema.
- La solución garantiza un nivel de aceptación rápido.
- La solución garantiza una transacción segura y con un tiempo de respuesta no menor de 5 seg.
- La solución hace uso de las siguientes herramientas de software:
  - Modulo IVR: software **CT ADE** y Tarjetas de Telefonía Digitales **Dialogic**.

- Modulo WAP: arquitectura de componente COM de Microsoft en un servidor WEB **Internet Information Server**, siendo esta una plataforma estable en otras soluciones WEB y WAP ya implementadas (por lo cual se ha desestimado alternativas como Apache, Personal Web Server, WebSphere, etc.).

- Sistema fácil de usar tanto para el comprador y vendedor.
- La solución implementa protocolo SSL de manera que garantiza la seguridad en las transacciones realizadas.
- La solución garantiza la seguridad en la transmisión de los datos mediante una red IP-VPN (VISA y Red de Móviles).
- La solución comprende las tecnologías WAP e IVR, por lo cual el comprador solo requerirá de un simple Terminal móvil digital (no WAP) para realizar operaciones.
- El Sistema hace uso de los módulos IVR con mensajes de voz cortos y claros de manera que el comprador pueda autorizar o rechazar las operaciones, además de poder consultar las operaciones realizadas desde su dispositivo móvil discando un número telefónico.
- El Sistema proporciona una pagina web de manera que el comprador y vendedor puedan consultar sus operaciones y cambio de clave.
- El sistema hace uso de la tecnología SMS para enviar confirmaciones de las operaciones al comprador y vendedor mediante mensajes de texto.
- Los módulos IVR del Sistema pueden migrar con facilidad a un sistema, en el cual el comprador y/o vendedor realizan las operaciones vía comandos de voz (reconocimiento de voz).
- Telefónica Empresas cuenta con experiencia en el desarrollo de soluciones WAP e IVR.
- La actualización de la tecnología del sistema esta garantizada

por al empresa proveedora del software.

- La implementación y el mantenimiento del Sistema están a cargo de Telefónica Empresas.

Desventajas

- No se cuenta con muchas implementaciones a nivel local.
- La administración del sistema se realiza mediante tres plataformas (WAP, WEB e IVR).
- Se requiere una plataforma de desarrollo y producción de las mismas características ante cualquier actualización o cambio en el Sistema.

3.3 Metodología de Solución

Para decidir la mejor alternativa de solución, se realizo el siguiente análisis:

Funcionalidad:

Permitió medir cuanta de la funcionalidad requerida podría ser cubierta por cada alternativa. Se uso los siguientes criterios para su cuantificación:

- Sistema fácil de usar.
- Sistema integral, de manera que cumpla todos los requerimientos funcionales.
- Sistema flexible y adaptable a las nuevas funcionalidades que aparezcan.
- Sistema orientado al usuario.

Disponibilidad:

Se considero los siguientes factores:

- Acceso a la información en cualquier momento y lugar.
- Sistema disponible las 24 horas los 7 días de la semana.

Costos:

Se considero los costos involucrados para obtener la solución:

- Costos de Licencias de Software.
- Costos de Hardware.
- Costos de Desarrollo del Sistema.
- Costos de Implantación.
- Costos de Servicio Post-Instalación.
- Otros Costos.

Tiempo de Desarrollo:

Se midió el tiempo en el cual se tendría el sistema trabajando con todas las funcionalidades requeridas, y con las mejoras necesarias. Se busco la alternativa con los tiempos de desarrollo e implantación óptimos.

Tecnología:

Se considero la importancia de contar con herramientas de última tecnología, y que además sean estables tecnológicamente, de manera que el sistema final sea robusto, no descuidando que el sistema final se adapte de manera flexible a los cambios futuros.

La evaluación tecnológica ayuda a dar un gran valor agregado al negocio, propiciando una ventaja competitiva.

Criterios	Peso	Alternativa 1	Alternativa 2	Alternativa 3
Funcionalidad	3	3	3	5
Disponibilidad	3	3	2	4
Costo	2	2	3	4
Tiempo Desarrollo	1	4	3	3
Tecnología	1	4	3	4
Total		**30**	**27**	**42**

Fuente: Elaboración propia con información de Telefónica Empresas

3.4 Toma de Decisiones

Entre los criterios de selección que se han considerados tenemos:

Peso	Criterios
3	Funcionalidad
3	Disponibilidad
2	Costo
1	Tiempo de Desarrollo
1	Tecnología

(*) Peso: 1 es de menor peso, 3 de mayor peso.

Al evaluar todas las alternativas bajo la calificación que se ha considerado, se opta por la Alternativa 3 "Sistema de Medios de Pagos usando Tecnología Móvil (IVR, WEB y WAP)", la cual según la información de la calificación tiene la mejor Funcionalidad y Disponibilidad, además de contar con el Precio y el Tiempo optimo para el desarrollo e implementación en comparación a sus demás alternativas. Finalmente se opto por la Alternativa 3 debido a la experiencia tecnológica en soluciones de tecnología WAP e IVR, además ser un sistema nuevo y diferente a implementar en el Perú.

3.5 Estrategias Adoptadas

El presente plan de trabajo del Proyecto se elaborado siguiendo la metodología del estándar internacional **ANSI/PMI 99-001 2000,** sugerida por el PMI(Project Management Institute) y se gestiono utilizando las herramientas y conceptos contenidos en dicho fundamento, considerado un estándar a nivel mundial para la dirección de proyectos.

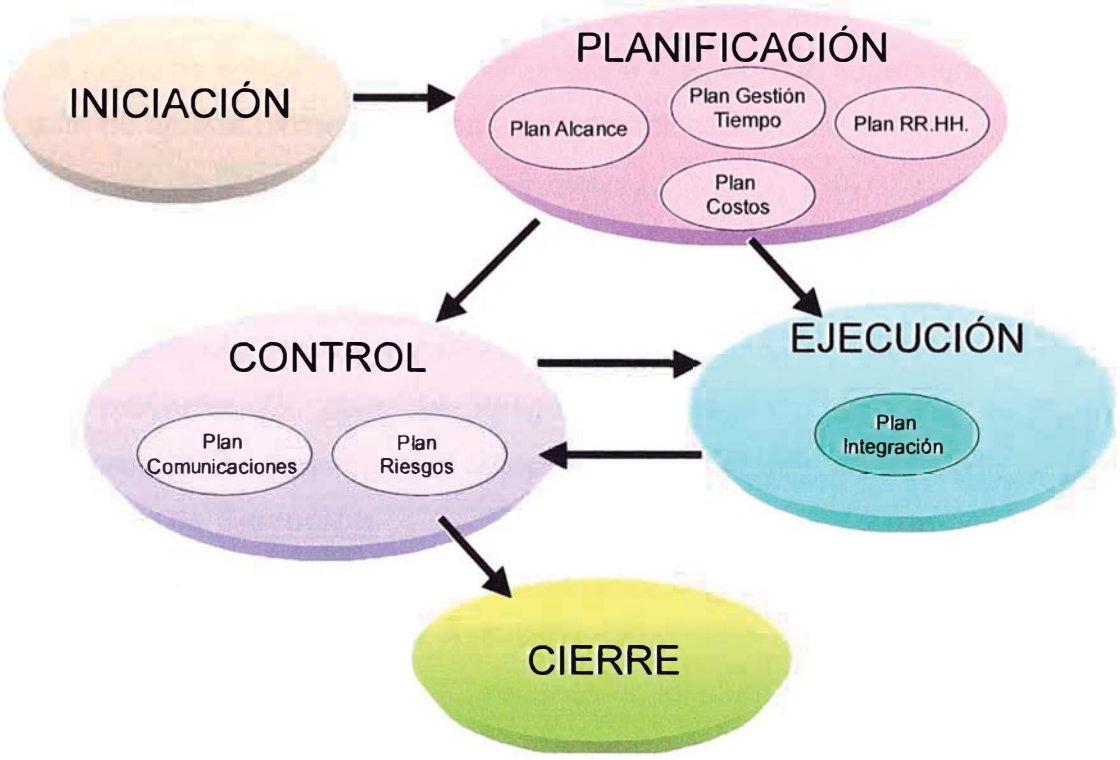


Fig. 10

A continuación se dará una breve explicación de los procesos de la metodología PMI que se involucraron durante todo el proyecto.

a. <u>Proceso de Iniciación</u>

El plazo del proyecto se iniciará con la firma del contrato. Luego se ejecutará un plan de procura o adquisiciones que permitirá efectuar la entrega de los bienes propuestos en el tiempo comprometido en el plan de gestión de tiempo.

b. <u>Proceso de Planificación</u>

La planificación es un proceso de análisis y descomposición de los procesos principales para asegurar el cumplimiento del cronograma, del presupuesto y la calidad del proyecto. Este proceso puede extenderse a lo largo de la ejecución del proyecto, no obstante, deberá generar los planes de Gestión del Alcance, Gestión de Tiempos, Recursos Humanos y Costos. Inicialmente se ajustarán los criterios utilizados en la

planificación del presente plan, luego se establecerán reuniones con personal técnico de los equipos de trabajo (equipo formados deacuerdo a los módulos a implementar: WAP, WEB e IVR, con un supervisor a cargo) a fin de ajustar últimos detalles y coordinaciones.

c. Proceso de Control

Contempla los planes de Comunicaciones y de Riesgos, que permitirán gestionar las coordinaciones y avances de los trabajos y actividades, de forma conjunta con los supervisores de los equipos de trabajos a lo largo del proyecto. El plan de riesgo permitirá mantener los alcances comprometidos y asegurar el cumplimiento del cronograma y WBS.

d. Proceso de Ejecución

Contempla la ejecución de las actividades, procesos y tareas definidas en el presente plan de trabajo. Asimismo comprende el desenvolvimiento del Plan de Integración, cuyos procesos involucran el despliegue de los planes de Alcance, Tiempo, Riesgos, y otros, descritos en el proceso de planificación.

Los avances y documentación relacionada con las instalaciones se irán canalizando y afinando con los equipos de trabajo. Posteriormente se coordinará con los equipos de trabajo un control de cambios a definirse.

e. Cierre del Proyecto

En esta fase del proyecto se firmará el acta de aceptación del sistema y se realizará la entrega de toda la documentación correspondiente a los equipos, manuales técnicos, manuales de usuario y manuales de mantenimiento del sistema.

El Plan desarrollado incluye y detalla todos los procesos y procedimientos requeridos para la implementación adecuada de los diferentes componentes del proyecto, asimismo exceder las necesidades y expectativas de los interesados del proyecto.

El Plan de Trabajo adicionalmente se tomo en cuenta la integración y coordinación de todos los planes de trabajo parciales del proyecto para crear un único documento consistente y coherente.

Los planes incorporados son:

a. Plan de Gestión de Alcance

Esta parte abarca la subdivisión de los principales entregables del trabajo en componentes más pequeños y manejables con el fin de mejorar la precisión de las estimaciones de costos, duración y recursos.

Aquí definimos los principales entregables del proyecto y definimos los alcances a través del uso del WBS[i], herramienta de descomposición de actividades (ver Fig. 8).

Una de las características principales del plan de gestión de alcance fue la definición la gestión de cambios lo cual fue muy importante para llevar a cabo el proyecto.

b. Plan Gestión de Cambios

Cualquier requerimiento que implique cambios en las funciones o características de los servicios descritos en la presente propuesta y que ocurran durante el proceso de implantación, serán tratados según el Procedimiento adjunto.

Un cambio podrá ser originado por iniciativa de cualquiera de las partes. Para asegurar un tratamiento uniforme, se usará el formato descrito en el Anexo Formato de Solicitud de Cambio.

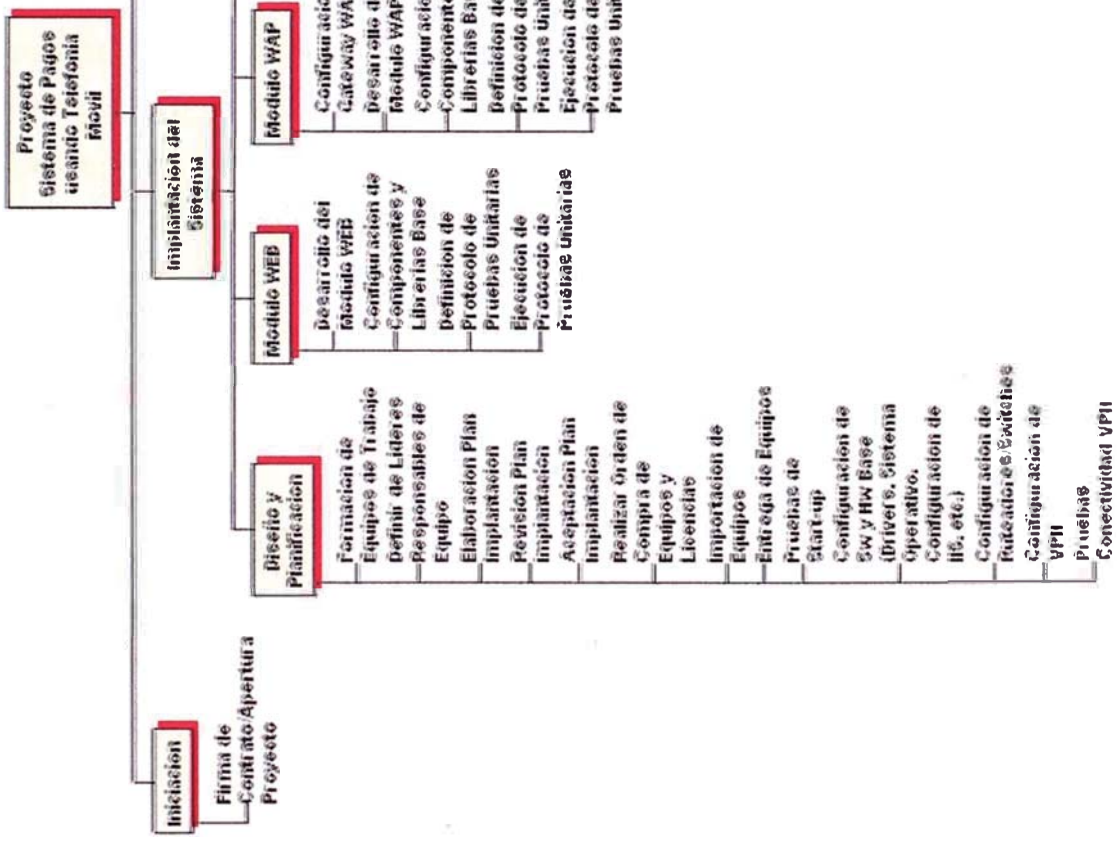

Proyecto
Sistema de Pagos
usando Telefonia
Movil
Iniciacion
Firma de
Contrato/Apertura
Proyecto
Implantacion del
Sistema
Diseño y
Planificacion
Formacion de
Equipos de Trabajo
Definir de Lideres
Responsables de
Equipo
Elaboracion Plan
Implantacion
Revision Plan
Implantacion
Aceptacion Plan
Implantacion
Realizar Orden de
Compra de
Equipos y
Licencias
Importacion de
Equipos
Entrega de Equipos
Pruebas de
Start-up
Configuracion de
Sw y Hw Base
(Drivers, Sistema
Operativo,
Configuracion de
IIS, etc.)
Configuracion de
Ruteadores/Switches
Configuracion de
VPII
Pruebas
Conectividad VPII
Modulo WEB
Desarrollo del
Modulo WEB
Configuracion de
Componentes y
Librerias Base
Definicion de
Protocolo de
Pruebas Unitarias
Ejecucion de
Protocolo de
Pruebas Unitarias
Modulo WAP
Configuracion del
Gateway WAP
Desarrollo del
Modulo WAP
Configuracion de
Componentes y
Librerias Base
Definicion de
Protocolo de
Pruebas Unitarias
Ejecucion de
Protocolo de
Pruebas Unitarias
Modulo IVR
Instalacion y
Configuracion de
Tarjetas Dialogic
Instalacion de Sw
de IVR : CT ADE
Configuracion de
Protocolo de
Señalizacion R2
Pruebas de
Start-up y
Comunicacion de
Señalizacion
Protocolo R2
Desarrollo de
Modulo IVR
Definicion de
Protocolo de
Pruebas Unitarias
Ejecucion de
Protocolo de
Pruebas Unitarias
Pruebas Integrales
Elaboracion de
Protocolo de
Pruebas
Revision de
Protocolo de
Pruebas
Aprobacion de
Protocolo de
Pruebas
Ejecucion de
Protocolo de
Pruebas
Desarrollo de
Manuales
Usuario Tecnico de
la Solucion
(Integracion de
Manuales)
Ajustes y
Correcciones
Cierre
Aceptacion del
Proyecto
Entrega de
Documentacion
Cierre de Proyecto
Entrega de
Proyecto a Area de
Post-Venta

Fig. 11

PROCEDIMIENTO DE GESTIÓN Y CONTROL DE CAMBIOS:

Cambios menores (MEJORAS).- Si el requerimiento está enmarcado en el alcance de lo establecido en la propuesta y no afecta los costos, ni los cronogramas o plazos de ejecución o su efecto es manejable.

El nivel de aprobación está a cargo de los Jefes de Proyecto y los Supervisores de Equipo.

Cambios moderados (CAMBIO).- Si el requerimiento está enmarcado en el alcance de la propuesta, pero afecta en costos menores y cronogramas de implantación de hasta 1 semana.

El nivel de aprobación está a cargo de los Jefes de Proyecto.

Cambios mayores (MODIFICACIÓN).- Si el requerimiento no está enmarcado en el contexto del presente documento o afecta sustancialmente los costos o cronogramas de implementación.

El nivel de aprobación se da a nivel de El nivel de aprobación está a cargo de los Jefes de Proyecto con información a las Gerencias Centrales cuando la magnitud del cambio lo amerite.

Para este caso, se observan las siguientes reglas:

- No podrá modificarse la naturaleza u objeto de la presente propuesta.
- No podrá alterarse o gravarse en grado tal que resulte excesivamente oneroso el cumplimiento a cargo de una de las partes.
- Deben mantenerse sustancialmente las condiciones técnicas de la presente propuesta.
- Debe reconocerse al Jefe de Proyecto, los nuevos costos provenientes de la MODIFICACIÓN de ser ésta aceptada.

La aprobación o no del cambio deberá realizarse en los siguientes plazos. Para las MEJORAS O CAMBIOS hasta 5 días hábiles después de recibida la solicitud. Para las MODIFICACIONES, hasta 30 días después de recepción de tal solicitud.

Finalmente complementamos el plan con la descripción y alcance de los servicios post-venta y garantías mencionados en el documento de la Propuesta Técnica

c. Plan de Integración

Se elaboro un presente plan de trabajo con el objetivo de cumplir ampliamente con los ENTREGABLES requeridos para el aseguramiento de la calidad.

La Solución es llave en mano, por lo cual Equipo de Trabajo, pondrá a disposición de todos los elementos necesarios para cumplir con los requisitos que solicitan en la presente proyecto.

Hito	Entregable	Sub-Entregable	Bienes y/o Servicios que comprende el entregable
I	PROCESO DE INICIACION		
	Firma del Contrato		
	Reunión de lanzamiento "Kick off"	Plan de Proyecto.	Elaboración de protocolo de Pruebas y Documentación (Topologías, diagramas, configuraciones, etc.).
	Entrega de Equipos		
II	PROCESO DE PLANIFICACION		
	Plan de Gestión Alcance		Importación de Bienes
	Plan de Gestión Tiempo		
	Plan de Gestión de Costos		Propuesta Económica elevada a los stakeholders
	Plan de Gestión RR.HH.		
III	PROCESO DE CONTROL		
	Plan de Comunicaciones		Metodología para las coordinaciones con los stakeholders y equipos de Trabajo.
	Plan de Riesgos		
IV	PROCESO DE EJECUCION		
	Plan de Integración		Desarrollo de todos los planes integrados
	Desarrollo e Implementación de Módulo WEB.		Desarrollo, Instalación, configuración y puesta a punto
	Desarrollo e Implementación de Modulo WAP		Desarrollo, Instalación, configuración y puesta a punto
	Desarrollo e Implementación de Modulo IVR		Desarrollo, Instalación, configuración y puesta a punto
	Cursos de Capacitación		Administración y Configuración del Sistema
V	PROCESO DE CIERRE		
	Ajuste y Cierre.		

d. Plan de Gestión de Riesgos

La estrategia básica de gestión de riesgos está orientada a identificar áreas críticas y eventos de riesgo y tomar acciones para manejarlos antes de que puedan generar problemas que impacten en el costo, tiempo o calidad.

Este plan contempla una evaluación estructurada para la identificación y análisis de los procesos y productos críticos, el desarrollo de alternativas de mitigación y la supervisión de la efectividad de las respuestas seleccionadas. Se establece un formato estándar de registro de riesgos que alimenta la base de datos de gestión de riesgos. En todas las revisiones del proyecto se revisarán los riesgos, a fin de mantener controlados los riesgos identificados y vigilar continuamente áreas que a futuro pueden impactar en el proyecto.

C	Área de Riesgo	Plan de Riesgo y/o Mitigación	Análisis Cualitativo
1	Ambiente Físico -Desastres -Infraestructura	Plan de actividad del Riesgo	
2	Paralización de actividades de algún ente tercero (Aduanas, Transporte, etc.)	Notificación a los stakeholders causa de Fuerza Mayor. Aplicación de Fast Tracking siempre que se encuentre en ruta crítica	Retardo en el tiempo de ejecución.
3	Huelgas, cierre de predios, cierre de carreteras, derrumbes.	Informar a los stakeholders con causa: Condición de Fuerza Mayor. Aplicación Crashing (mayor número de horas de trabajo)	Retardo en el tiempo de ejecución.
4	Impedimento acceso a Ambientes por condiciones climáticas extremas.	Notificar formalmente condición de Fuerza Mayor a las Gerencias correspondientes.	Retardo en el tiempo de ejecución.
5	No contar con personal de apoyo de Telefónica Móviles o Data Center.	Se efectuarán coordinaciones sucesivas durantes las 24 horas posteriores. De continuar situación se informará a la Gerencia responsable de Telefónica Móviles o el Data Center.	Retardo en el tiempo de ejecución.
6	No cumplir los Hitos propuestos	Se aplicarán las herramientas de fase Tracking y Crashing de ser necesario	Mayor costo. Retraso en el tiempo de entrega.
7	Falta de Material para la Instalación	Control estricto por cada instalación. Activar disparadores	Retraso en tiempo de entrega. Penalidades.

e. Plan de Gestión de Recursos Humanos

El cual se presenta la Organización del Proyecto, estructurado de acuerdo a las necesidades del concurso. (Jefe de Proyecto, Especialistas y personal de apoyo).

Asimismo se incluye un **Plan de Gestión de Tiempos**, el cual incluye el Cronograma, detallando los tiempos de ejecución de las actividades definidas en el alcance.

EQUIPO DE TRABAJO:

- **Jefe de Proyecto:** Experto en Soluciones de Comunicaciones.
- **Supervisor 1:** Experto en Soluciones WEB.
- **Supervisor 2:** Experto en Soluciones WAP.
- **Supervisor 3:** Experto en Soluciones IVR.
- **Especialistas 1, 2 y 3:** Técnicos en Soluciones WAP, WEB e IVR.
- **Stakeholders:** Telefónica Empresas, Telefónica Móviles, VISA Perú.

f. Plan de Gestión de Comunicaciones

En el cual se describe las formas de comunicaciones entre los diferentes miembros del proyecto y los formalismos del caso.

- **Llamada Telefónica:** Ante cualquier evento o coordinación fuera de las reuniones establecidas se hará uso de la llamada telefónica como medio de comunicación.
- **Correo Electrónico:** En casos de cambios de alcance o coordinaciones formales se sugiere el uso del correo electrónico en esas circunstancias.

Dentro del plan de comunicaciones fue muy importan te la definición de toda la documentación que se iba manejar durante el proyecto.

f.1. Requerimientos de Información

- **Documentación de implantación del proyecto:** Todos los trabajos de gestión e implantación del proyecto se efectuarán en base a la siguiente documentación:

  Cuestionario de levantamiento de información de la situación actual de equipos existentes.

  Informes de replanteo (en caso aplique)

- Plan de numeración o direccionamiento (en caso aplique).
- Plan de Implantación
- Cronograma de Implantación
- Informe de seguimiento y revisión de avance del Proyecto
- Protocolo de Pruebas Parciales
- Protocolo de Pruebas Globales.
- Informe de parámetros de configuración finales.

Las versiones preliminares de todos estos documentos serán sometidas a la revisión aprobación de los stakeholders.

- **Recomendaciones de seguridad durante las instalaciones:** Elaborar una documentación de acciones para mantener una adecuada seguridad en las áreas de trabajo como: señalización, limpieza y procedimientos que aseguren la integridad fisica de las personas.
- **Elaborar documento para establecer las reuniones de trabajo con el cliente y los stakeholders :** Se planteará el siguiente esquema de reuniones:
  - 1er Mes – Una (1) reunión por semana
  - 2o Mes – Dos (2) reuniones por semana
  - 3er Mes – Dos (2) reuniones por semana
  - 4o Mes – Dos (2) reuniones por semana y las que se considere necesarias para la aceptación final del Proyecto.
- **Documentación de fin del proyecto :** Entre los documentos a ser provistos una vez finalizado el proyecto tenemos:
  - Fuentes de los Programas
  - Manuales de Operación
  - Manual de Sistema
  - Manual de Seguridad
  - Manual de Usuario
  - Otros Elementos necesarios para la ejecución y mantenimiento de la solución.
  - Manuales de desarrollo, arquitectura y de datos.

- Especificaciones técnicas de los equipos suministrados.
- Planos y diagramas topológicos.
- Informe final de implantación.
- Formatos (actas) parciales o totales de conformidad de puesta en producción para cada uno de los entregables del proyecto.
- Resultados a pruebas de funcionamiento.

g. Plan de Gestión de Costos

Las estimaciones y planes para la gestión de costos fueron integradas en la Propuesta Económica

CAPITULO IV
EVALUACIÓN DE RESULTADOS

El resultado que se obtuvo después de haber implementado el sistema fueron excelentes, a pesar de haber sido la primera implementación del grupo al cual forme parte integral de la Gerencia de Soluciones y ASP Hosting, inclusive después de la implementación se implementaron nuevas funcionalidades orientadas al negocio B2C, lo cual la plataforma pudo soportar dichas funcionalidades sin impactar en la solución inicial.

En resumen los resultados obtenidos fueron:

Transacciones realizadas. En los primeros dos meses se realizaron un 20% de las transacciones que se habían proyectado.

Adaptabilidad. En los primeros dos meses se noto una rápida aceptación del sistema por parte de los compradores y vendedores.

Mejora en el Proceso. Se vio una gran mejora en el proceso de compras, debido a que los negocios ofrecían diferentes planes de pagos y ofertas.

Aceptación del Sistema. En un primer momento fue utilizado por un negocio, el cual se adapto rápidamente al sistema. Actualmente se están implementando nuevas funcionalidades el cual hace el sistema más configurable.

Nuevo Esquema de Trabajo. Hacer uso de la metodología PMI, nos permitió llevar un mejor control de las actividades así como manejar los costos.

Durante el proceso de evaluación (económica) se preparo un cuadro con las estimaciones de flujo de caja, para el análisis ROI se considero los siguientes costos:

- Ingresos (Costo por Transacciones a facturar).
- Costos de Implementación (Horas Hombre, Hardware, Software).
- Costos de Soporte y Mantenimiento (por parte de Telefónica).
- Costos de Soporte y Mantenimiento del Fabricante.
- Costos de Actualización de la Plataforma.
- Costos de Depreciación.
- Impuestos.

Costo	Valor
Licencias Software	41,800.00
Equipos Servidores	28,000.00
Equipos Comunicaciones	12,900.00
Comunicaciones	1,300.00
Implementacion	28,000.00
Total Proyecto (USD)	**112,000.00**

Costos \ Periodo	Año 1	Año 2	Año 3
Ingresos(x Transacciones)	198964.08	340296.10	582021.81
Costo Soporte y Mantenimiento	107520.00	107520.00	107520.00
Costo Soporte Fabricante	67200.00	67200.00	67200.00
Costo Actualizacion	11200.00	11200.00	11200.00
Depreciacion	2000.00	2000.00	2000.00
Utilidad Operativa	11044.08	152376.10	394101.81
Impuesto	4622.26	45712.83	118230.54
Utilidad Neta	6421.83	106663.27	275871.27

Tasa Interes	0.12
Tasa Interes COK(Inversionistas)	0.18

Periodo	Año 1	Año 2	Año 3	Total (USD)
Utilidad (USD)	6421.83	106663.27	275871.27	
VAN	5733.77	85031.31	196359.72	**287124.80**
VAN(COK)	5442.23	76603.90	167903.77	**249949.90**

VALOR PROYECTO AÑO 0 :	USD 112000	
INDICADORES DE RENTABILIDAD		
VAN	287124.80	**Proyecto Aceptable**
VAN(COK)	249949.90	**Proyecto Aceptable**
Interes	0.12	
Interes(COK)	0.18	
TIR	0.31	**Proyecto Aceptable**
TIR(COK)	0.24	**Proyecto Aceptable**

Fuente: Elaboración propia con información de Telefónica Empresas Peru S.A.C.

Finalmente deacuerdo a la tabla mostrada se muestra un proyecto rentable en un flujo de caja de tres años, además de un tiempo de dos años para la recuperación del capital invertido (proyección considerada inicialmente).

CAPITULO V
CONCLUSIONES

Las principales conclusiones son las siguientes:

- La implementación de este nuevo sistema permitió a Telefónica Empresas encontrar un nuevo nicho de mercado y una ventaja competitiva.
- La metodología PMI esta siendo usada para todos los proyectos de Telefónica Empresas, la cual se ha ajustado a todos los tipos de proyectos que maneja Telefónica Empresas.
- Nos permitió conocer mejor el mercado actual peruano, ya que se determino una necesidad y se planteo la mejor solución accesible al mercado peruano.
- Nos permitió desarrollar una solución que no solo se hizo uso de los recursos de Telefónica Empresas, sino de otras empresas de Grupo.
- La implementación del Sistema ayudo a demostrar que la empresa se encuentra en capacidad de implementar nuevas soluciones.
- Una vez que se termino la implementación del sistema se procedió ha realizar una revisión del proyecto, el cual sirvió como modelo para otros nuevos proyectos.
- La experiencia y/o habilidad en la formación del equipo de trabajo fue importante durante el desarrollo del producto para obtener un correcto resultado en el producto final.

CAPITULO V
RECOMENDACIONES

Las principales recomendaciones son las siguientes:

- Se recomienda considerar todos los escenarios posibles durante las pruebas integrales, esto permite minimizar los ajustes del sistema en producción.
- Para mantener el proyecto bajo control, se recomienda considerar todos los riesgos en el proyecto y no solo a nivel de desarrollo de la solución.
- Para que los acuerdos y la comunicación sea efectiva, es importante que todos los responsables del proyecto se encuentren involucrados durante todo el proyecto.
- Se recomienda realizar un protocolo de pruebas de manera integral que incluya desde comunicaciones hasta el software final de usuario.
- El apoyo de la gerencia al proyecto permite que la organización en sí se comprometa con el mismo, se recomienda contar con el apoyo de la gerencia como un factor muy importante dentro de una implantación.
- Se recomienda definir desde un principio las políticas y canales de comunicación e informar a todos los miembros del proyecto acerca de los mismos. Asimismo, revisar que durante el proyecto, la utilización de dichos canales sea óptima (Metodología PMI).

GLOSARIO DE TERMINOS

IVR : Sistema de Respuesta de Voz vía teléfono, en muchos casos son conocidos como operadoras automáticas.

POS : Terminal electrónico para realizar pagos mediante tarjetas bancarias ATM de debito y/o crédito.

HTTP : Protocolo de Transferencia de Hipertexto.

HTTPS : Protocolo Seguro de Transferencia de Hipertexto.

BWS : Es una estructura de árbol jerárquica de tareas o entregables que necesitan ser ejecutadas para que un proyecto sea completado.

ORACLE : Nombre de software de Base de Datos.

VISUAL BASIC : Nombre de software, el cual es usado para desarrollar y crear programas.

DIALOGIC : Marca de Tarjeta de Telefonía.

BIBLIOGRAFIA

- PC Telephony.
  Bob Edgar, 4° Edicion, Edit. CMP Books, New York, 1997.
- A Guide to the Project Managment Body of Knowledge (PMBOK Guide).
  Project Managment Institute , 3° Edicion, Edit. Project Managment Institute, 2004.
- SSL & TLS Essentials: Securing the Web.
  Stephen A. Thomas, 1° Edicion, Edit. Wiley; Bk&CD Rom edition, 2000.
- SSL and TLS: Designing and Building Secure Systems.
  Eric Rescorla, 1° Edicion, Edit. Addison-Wesley Professional, 2000.
- VoiceXML.
  Chetan Sharma, Jeff Kunins, 1° Edicion, Edit. John Wiley & Sons, Inc., New York, 2002
- Intel Web.
  www.intel.com/design/network/products/telecom/index.htm
- Envox Web.
  www.envox.com
- Dialogic Web.
  www.dialogic.com

ANEXOS

ANEXO 1

1 Sistemas de encriptación en SSL

1.1 Sistema de encriptación de clave simétrica

La encriptación y descifrado con claves simétricas (la misma clave) es entre 10 y 100 veces más rápido que un algoritmo de claves asimétricas (distintas).

El esquema habitual de trabajo con claves simétricas es el siguiente:

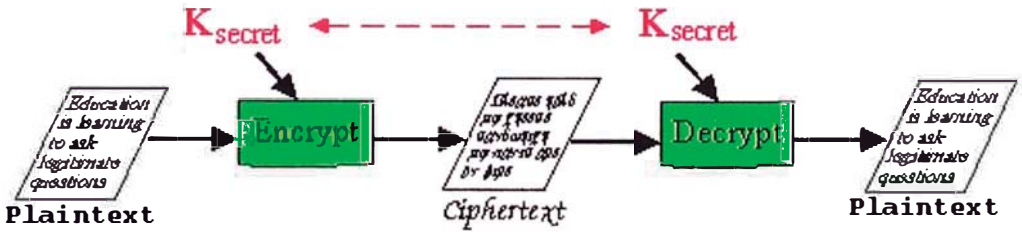


Fig. 12

En esta imagen, un texto "plain text" es transformado según una clave (Ksecret), trasferido, y desencriptado con la misma palabra clave. Esta clave debe haberse sumnistrado por un medio seguro al receptor, de manera que no haya sido "capturada", si la clave llega a manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha clave y generar una nueva. El problema que se plantea es ¿por qué medio trasmite A la clave a B?

Algoritmos simétricos mas comunes

Los algoritmos simétricos se clasifican en algoritmos para bloques de texto o flujo de datos. Los primeros trabajan sobre un grupo o bloque de bytes, en tamaños definidos; los segundos encriptan byte a byte toda la información.

DES: Adoptado como estándar ANSI en 1977. En una técnica de cifrado sobre bloques de texto que usa claves de 56 bits.

DESX: variación del DES; introduce un proceso de encriptado en dos fases que hace prácticamente imposible encontrar la clave.

Triple-DES: Algoritmo DES pero utilizando tres claves distintas. Este algoritmo es el más utilizado en transacciones en instituciones financieras.

RC2: Sistema de cifrado en bloques adoptado inicialmente por la agencia RSA; admite claves con longitudes entre 1 y 2048 bits. La versión de exportación limita su uso a claves de 40 bits. Desarrollado por Ronald Rivest.

RC4: Sistema de cifrado de flujo, también adoptado por por la agencia RSA; admite claves con longitudes entre 1 y 2048 bits. La versión de exportación limita su uso a claves de 40 bits. Desarrollado por Ronald Rivest en 1994.

RC5: Sistema de cifrado en bloques adoptado inicialmente por la agencia RSA; admite claves con longitudes entre 1 y 2048 bits. Permite que el usuario varíe el tamaño del bloque que se encripta en cada paso. Desarrollado por Ronald Rivest.

¿Es descifrable un mensaje encriptado con clave simétrica?

Para un algoritmo probado, como es el RC4, el problema de la seguridad depende de la longitud de la clave. Para claves de 40 bits de longitud, hay 2^40 claves posibles (1,1x10^12). Un ordenador podría tardar unas horas en conseguir la clave; si se emplea una clave de 128 bits, las claves posibles son 2^128 (3,4x10^38), y el tiempo necesario para averiguar la clave sería del orden de la edad del universo (1,8x10^10 años).

Estos datos suponen que se trata de un ataque del tipo ensayo-error. Con métodos más refinados, por ejemplo, si se conoce parte del texto encriptado, el proceso de búsqueda puede refinarse y acortarse.

1.2 Sistema de encriptación de clave asimétrica

Los algoritmos asimétricos basados en claves distintas (normalmente dos llaves) son lentos pero tienen la ventaja de que una de las claves puede ser conocida por cualquiera; el mensaje encriptado por esa clave "pública" sólo puede ser descifrado por la otra clave, privada, conocida sólo por el destinatario: de ahí el término asimétrico. La llave pública es conocida por cualquiera; la privada sólo es conocida por el receptor.

Fig. 13

Si A desea enviar un mensaje a B, A encripta el mensaje con la clave pública (KB,public) de B; al recibir el mensaje, B lo descifra con su clave privada (KB,private).

Por el contrario, si B desea enviar un mensaje a A, B encripta el mensaje con la clave pública (KA,public) de A; al recibir el mensaje, A lo descifra con su clave privada (KA,private).

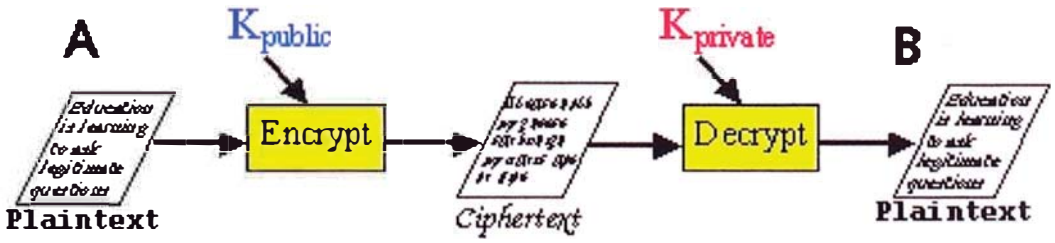


Fig. 14

Algoritmos asimétricos mas comunes

La característica básica de estos sistemas es que hay dos claves: la pública y la privada. La clave pública se genera a partir de la clave privada. Los principios de esta técnica han fueron desarrollados por Diffie y Hellman (Stanford University, 1975). Como estos algoritmos siempre

presuponen la existencia de una clave pública, se les denomina también sistemas de llaves públicas.

Los algoritmos asimétricos se clasifican en algoritmos para bloques de texto o flujo de datos. Los primeros trabajan sobre un número de bytes, en tamaños definidos; los segundos encriptan byte a byte toda la información.

Los algoritmos más utilizados son los siguientes:

Diffie-Hellman key exchange: propiamente es un sistema para generar e intercambiar una llave compartida por un canal no seguro.

RSA: Sistema de claves públicas desarrollodo por Rivest, Shamir y Adleman (MIT). Es utilizado tanto para encriptar información como para firma digital. Los sistemas de firma digital se utilizan para garantizar que el autor de la información es el firmante (es decir, que la información no ha sido modificada por un tercero). La clave puede tener una longitud variable y puede ser tan grande como se desee.

DSS: El sistema de firma digital (digital signature system) fue desarrollado por la Agencia de Seguridad Nacional de los EE. UU. (NSA) y puede utilizar claves entre 512 y 1024 bits de longitud..

La seguridad de estos sistemas depende de la longitud de la clave.

1.3 Sistema de transmisión seguro basados en la utilización conjunta de clave pública y privada

Los sistemas de transmisión de claves (Difie-Hellman) utilizan combinados ambos algoritmos de encriptado: la criptografía asimétrica (step 1) para transferir la clave simétrica (Ks), y la criptografía simétrica -mucho más rápida- para transferir la información. La clave simétrica (Ks) se transfiere encriptada en la primera fase, pues es necesaria para encriptar/desencriptar el flujo de datos posterior.

Paso 1 (step 1): A genera la clave simétrica (Ks) que deben utilizar A y B en sus transmisiones en esa sesión. Las razones para utilizar una clave simétrica son la velocidad y que, para mayor seguridad, se genera para el caso. Para enviar esta clave de manera segura a B, A utiliza la clave asimétrica pública de B (Kb, public); cuando B recibe la clave Ks encriptada

con su clave pública, la descifra con la clave asimétrica privada (Kb, private) que sólo posee B.

Paso 2 (step 2): Una vez que A y B poseen la misma clave simétrica (Ks) la transmisión se realiza encriptando toda la información con esa clave en ambos sentidos.

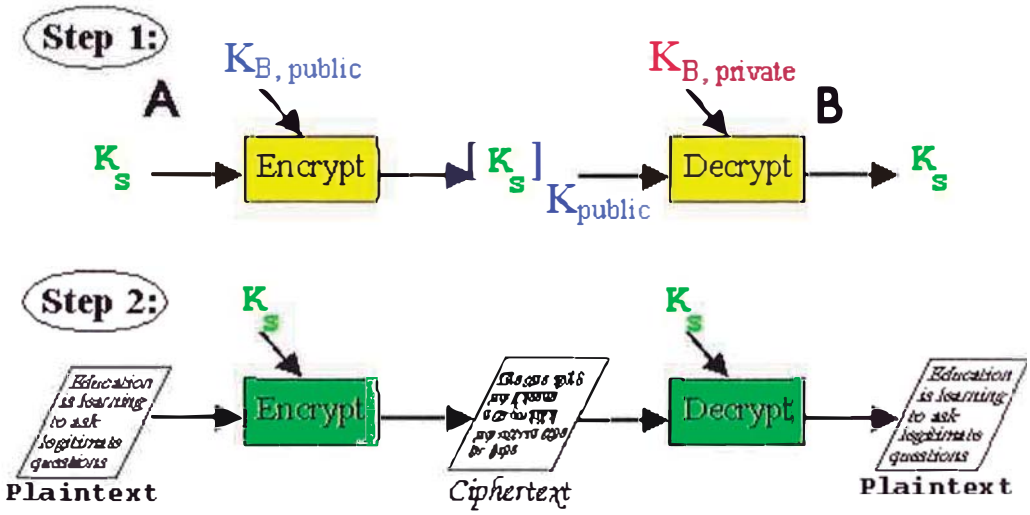


Fig. 15

1.4 Digest

Un digest es una función matemática que produce una secuencia de caracteres, normalmente entre 128 y 256 bits de longitud, a partir de un archivo de información inicial de cualquier longitud.

Los digest tienen las siguientes propiedades:

- Cada bit de salida del digest es influenciado por cada bit de entrada.
- Para cualquier bit que se cambie a la entrada, cada bit de salida tiene al menos un 50% de probabilidades de cambiar.

Dado un fichero (texto) de entrada, debe ser informáticamente inviable encontrar otro texto de entrada que del mismo producto en el digest.

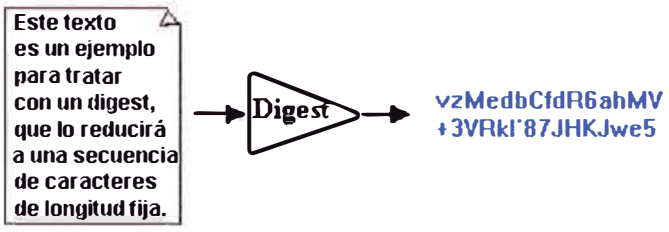


Fig. 16

Las funciones digest más utilizadas son las siguientes:

HMAC: Hassed Message Authentication Code, usa -además- una clave secreta.

MD2: Message Digest #2, desarrollado por Ronald Rivest, produce un digest de 128 bits, aunque requiere bastante tiempo para calcularse.

MD4: Desarrollado por Ronald Rives como alternativa al MD2. Ha resultado ser un tanto inseguro.

MD5: Más seguro que el MD4. También genera un digest de 128 bits.

SHA: Desarrollado por la NSA, produce un digest de 160 bits.

Además, siempre es posible utilizar un digest dentro de un mensaje y encriptar el digest con una clave; de esta forma se puede firmar digitalmente el mensaje. También se utilizan para generar claves a partir de frases; de este modo el usuario no tiene que recordar una clave compleja, ilegible y larga (condiciones para que sea segura), si no una frase tan larga (y familiar) como quiera, que es transformada por un digest en su clave para descifrar.

1.5 Infraestructura de llaves publicas

Los sistemas de llaves públicas requieren que cada usuario genere dos claves, una pública y una privada. Estas claves tienen las siguientes propiedades:

La clave privada, se usa para desencriptar los mensajes recibidos y para firmar digitalmente.

La clave pública, se utiliza para enviar mensajes encriptados al usuario propietario de la llave y para verificar la firma digital del usuario propietario.

Las claves son bloques de caracteres ilegibles. A continuación se puede ver un ejemplo de una clave pública:

Type Bits/KeyID Date User ID

pub 1024/4C1FD235 1997/07/24 Pepe Díaz <pepe@unav.es>

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6.3ia

mQCNAzPXHYIAAAEEANRSmmsSkdLQMfRmjsVYdV63NTQvKNEtclT9Jw

EQebuyXFds

24JSj8pLbqOfxZYFZYe9c5uY6PjmiYMRz5yGdNYrEwXi30TwQVi9s/ZHi+sez
kqN
PdYJZ7Yt6CpIEDEV5BrZXKWHd5KSk/CV0Q+Slu/eImFS9jRic4svJ1NMH9I1
AAUR
tDBMdWNpYSBkZSBsYSBJZ2xlc2lhIDxsaWdsZXNpYUBtYWlsMi5jdGkudW
5hdi5l
cz6JAJUDBRAz1x2Diy8nU0wf0jUBAYg1A/98Oy4fHbw3MriQjt5KrqMmsOYA
xXyA
iEz2MYYZI2aSrzyzibkFbCKeMXL73Zp067Ifa7LLC/F5QWkzRCBhJNIXCwHk
fkD2
ti0AZsO/qttN1RGQjNNUkEJMQ31HunyEvQfc9bxsj2nPy661lhrTmntBVoFbp/j
6
g9/5nOM4VnjIDA==
=6IT8
-----END PGP PUBLIC KEY BLOCK-----

La clave pública es la que el usuario distribuye a todo aquel que quiera enviarle un mensaje cifrado. No hay ningún peligro en dejar a la vista la clave pública, ya que con ella sólo es posible encriptar mensajes. Lo importante es mantener bien guardada la clave privada porque con ella -y sólo con ella- es posible descifrar los mensajes enviados.

Un mensaje cifrado con una llave pública, sólo puede ser descifrado con la llave privada que generó la llave pública. Por lo tanto una llave pública sirve para codificar un mensaje y la privada para descodificarlo. Para mayor seguridad, el mensaje se codifica en relación al mensaje que se escribe, de manera que no es posible a partir de la clave pública y un texto encriptado reconstruir la clave privada en un tiempo asequible para un ordenador.

ANEXO 2

2 Descripción Técnica

2.1 Arquitectura IVR

Hardware

01 Servidor Pentium III/800 MHz 512 MB RAM
20 GB HDD CD-ROM 48X
Monitor 14", disk 3.5", keyboard, mouse
Bus de Expansión: 4 PCI / 9 ISA / 2 CPUs Slots
300 W Redundant Hot Swappable

01 Tarjetas de Interfaz Telefónica D/300 PCI-E1 (01 PRI)

Software

01 S.O Windows 2000 5 CLT

30 Licencias Software CT ADE

01 Oracle Client 8i

01 SQL Server 2000 Standard

Otros datos

Aplicacion IVR	CT ADE
Lenguaje de Programación	Scripting CT ADE
Base de Datos	Oracle 8i, SQL Server 2000

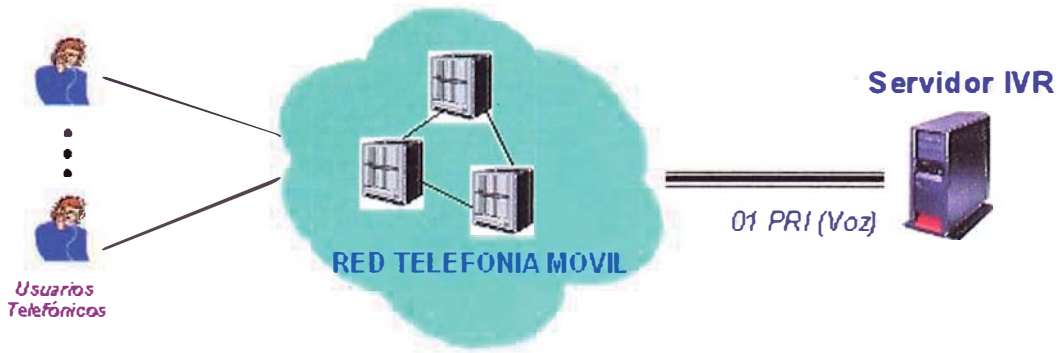


Fig. 17

2.2 Arquitectura WAP

Hardware

01 Servidor Pentium III/800 MHz 512 MB RAM
20 GB HDD CD-ROM 48X
Monitor 14", disk 3.5", keyboard, mouse
Bus de Expansión: 4 PCI / 9 ISA / 2 CPUs Slots
300 W Redundant Hot Swappable

Software

01 S.O Windows 2000 5 CLT

01 Internet Information Server 5.0

01 Oracle Client 8i

Otros datos

Aplicacion WAP	Internet Information Server 5.0
Web Server	Internet Information Server 5.0
Lenguaje de Programación	ASP HDML HTML JavaScript
Componentes COM	Visual Basic 6.0
Base de Datos	Oracle 8i

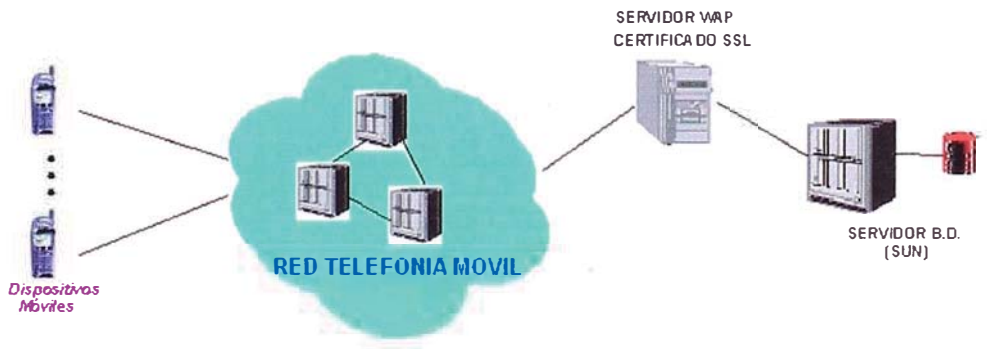


Fig. 18

ANEXO 3

3 Descripción Funcional

3.1 Proceso de Afiliación

- El usuario comprador/vendedor se acerca a la oficina de inscripción o afiliación con sus documentos respectivos (el tipo de documentos dependerá si el usuario es comprador o vendedor).
- El usuario entrega los documentos correspondiente al ejecutivo del servicio.
- El ejecutivo del servicio procede a llenar el formulario haciendo uso de la página web del sistema, el ejecutivo realiza una verificación previa de los documentos recibidos (verificación visual).
- Una vez que el ejecutivo del servicio llena toda la información del usuario solicitante, genera un número de fólder electrónico, este número es entregado al usuario para su posterior alta.

Fig. 19

3.2 Proceso de Alta

- Una vez que el usuario es registrado en el sistema como **Afiliado**, se procederá a realizar una revisión de toda la información entregada por el usuario (verificación de tarjetas de crédito, documento de identidad, estado de cuenta, etc.).
- Una vez que la información es terminada de revisar de procederá a enviar una carta, esta carta indicara si el usuario podrá se dado de alta o caso contrario se le indicara que no cumple con los requisitos para hacer uso del servicio.
- En caso el usuario sea dado de alta, recibirá una cuenta de usuario y una clave, además de una dirección web, desde la cual podrá hacer el cambio de su clave (el sistema obligara a que el usuario realice el cambio de clave por seguridad).

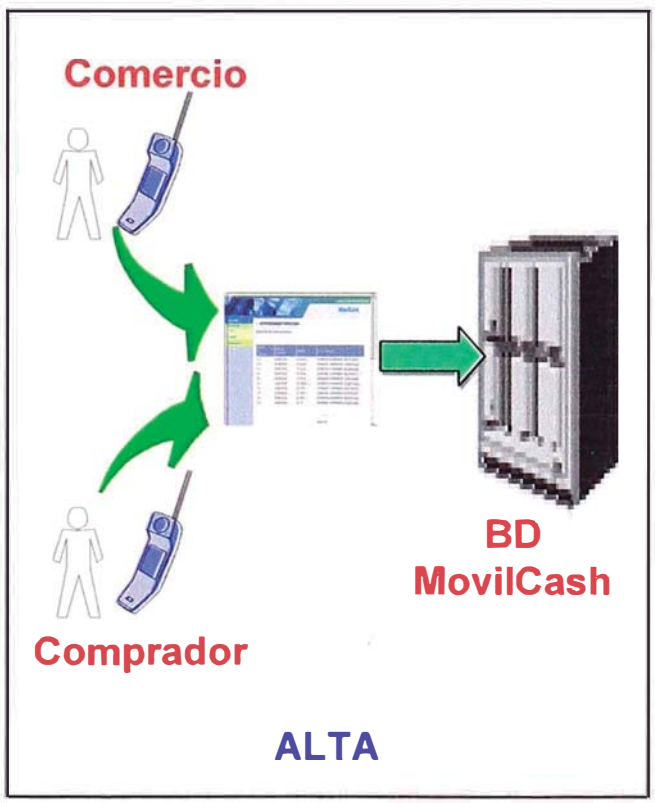


Fig. 20

3.3. Proceso de Compra

- El vendedor se conectara desde su dispositivo móvil al sistema de medios de pagos, haciendo uso de la opción WAP de su dispositivo móvil (el vendedor se deberá autenticar al sistema ingresando su usuario y password).
- El vendedor ingresara los datos de la operación en el dispositivo móvil.
- Una vez que el vendedor termine de ingresar los datos de la operación, el sistema de medios de pagos realizara una llamada al comprador.
- El sistema de medios de pagos indicara al comprador desde el dispositivo móvil, los datos de la operación.
- El sistema de medios de pagos, solicitara la confirmación de la operación, si el comprador se encuentra deacuerdo ingresara el numero de PIN el cual será solicitado por el sistema vía vocal.
- Una vez que el comprador autorice la operación, el sistema de medios de pagos enviara un mensaje SMS al celular indicando que la operación fue aceptada por el comprador o rechazada si no cuenta con el saldo suficiente.

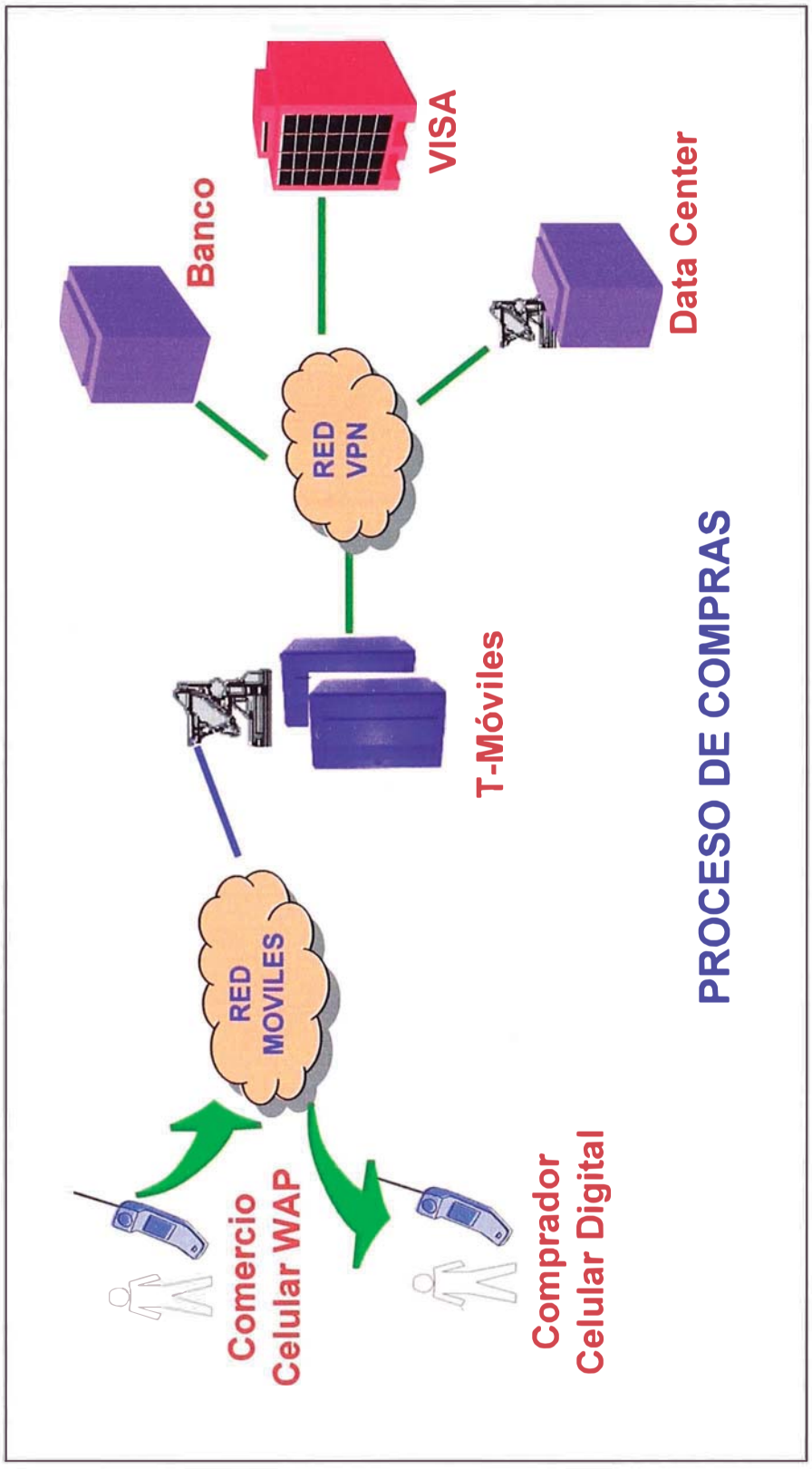

PROCESO DE COMPRAS
Banco
VISA
Data Center
RED VPN
T-Móviles
RED MOVILES
Comercio Celular WAP
Comprador Celular Digital

Fig. 21

ANEXO 4

4. Topología

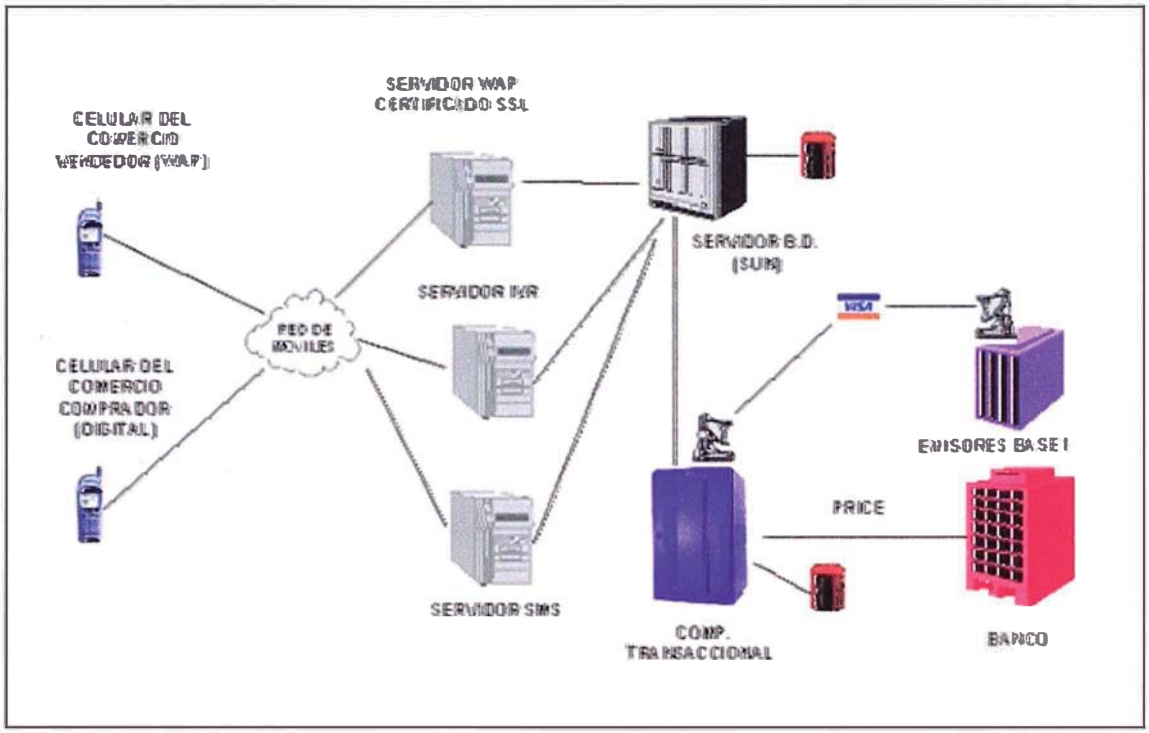


Fig. 22