ESCUELA POLITÉCNICA DEL EJÉRCITO
SEDE LATACUNGA

FACULTAD DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

PROYECTO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA:

IMPLANTACIÓN DE UN ASP (APPLICATIONS SERVICE PROVIDER) ORIENTADO A LA HOTELERÍA Y TURISMO

ELABORADO POR:

LUIS ORLANDO CHAMORRO SÁNCHEZ

LATACUNGA – ECUADOR
AGOSTO 2002

Capitulo

1

I.- DEFINICIÓN DE VENTAJAS Y CARACTERÍSTICAS QUE OFRECE UN ASP (APPLICATION SERVICE PROVIDER)

Un ASP proveer de aplicaciones a varios usuarios sea vía Internet o redes privadas, el alto costo de algunas aplicaciones hace que las pequeñas y medianas empresas no puedan acceder a estas, razón que ha ocasionado el desarrollo de los ASP, bajo este paradigma las empresas solo se dedican a su *core business* es decir a su actividad intrínseca, ya no se debe de preocupar de comprar TI, estar a la vanguardia de la tecnología o realizar actualizaciones de sus aplicaciones, el ASP provee a la empresa de las aplicaciones, actualización de las mismas y la empresa *solamente paga por uso,* un ASP es la mejor opción para poder acceder a sistemas sofisticados que tiene costos de Hardware y Software elevados.

1.1.- FUNDAMENTOS DE UN ASP

Los ASP son empresas de servicios que despliegan, alojan, implementan, y soportan aplicaciones desde un centro que funciona a lo largo de una red de área extendida (World Area Net - WAN), como por ejemplo Internet o una red privada virtual (Virtual Private Net - VPN). Los usuarios acceden desde grandes distancia a las aplicaciones utilizando Internet o líneas alquiladas. Un ASP generalmente agrupa servicios para permitir que el cliente interactúe con un solo punto de contacto y no con una colección de proveedores y tecnologías.

El alto costo de algunas aplicaciones ha ocasionado esta tendencia, razón por la cual Hewlett Packard y SAP han desarrollado el concepto de "cibercentros" que sirvan aplicaciones a otras compañías. Microsoft está permitiendo que algunas empresas ofrezcan sus productos de BackOffice incluyendo el SQL Server, Exchange y Windows NT como un servicio de alquiler y de pago por uso mientras que la forma común como los ASP están concebidos para proveer aplicaciones y servicios a las pequeñas empresas, las grandes empresas están utilizando el mismo concepto y tecnologías para proveer servicios a sus filiales.

Los ASP son muy parecidos a lo que hace 15 ó 20 años eran los mainframes de alquiler compartido grandes centros de procesamiento en los que se ejecutan aplicaciones para los clientes pero a diferencia de aquellos años, la oferta de aplicaciones de los ASP actuales va desde aplicaciones comunes de oficina como hojas de cálculo, pasando por servicios de correo electrónico, automatización de fuerzas de ventas o complejas aplicaciones de análisis financiero.

El público objetivo de los ASP son las pequeñas y medianas empresas, que podrán acceder a software de calidad y servicios que de forma tradicional es decir comprando, instalando, gestionando y manteniendo internamente no podrían acceder. La propuesta de valor para estas empresas se basa en que el ASP le proveerá de sus necesidades informáticas, de la misma manera que la compañía eléctrica lo hace con el suministro de energía.

Usando otra analogía se puede comparar con un proveedor de servicios de telefonía, ejemplo Andinatel es decir, todos tenemos la necesidad de utilizar un teléfono, ya sea en nuestra casa u oficina, y para hacerlo contratamos los servicios de una empresa suministradora, ya que resultaría imposible tener nuestro propio servicio, por los altos costos, infraestructura, entre otros; de tal forma que entre todos los subscriptores con un valor determinado cubrimos el costo por los servicios que

dicha compañía nos ofrece, cuando requerimos de algún soporte técnico o aclaración acudimos a ellos para su solución, de forma similar operan los APS con sus clientes.

Solo de esta manera las pequeñas empresas que son la mayoría en nuestro país podrán enfrentar los retos que este nuevo milenio les depara ya que si no cuentan con soporte técnico y soluciones informáticos, ellas no podrán sobrevivir.
Un ASP es la mejor opción para poder acceder a sistemas sofisticados, que tienen costos de hardware y software elevados.

Según datos de IDC, el mercado global de las ASP bordea los 150 millones de dólares anuales, previéndose un crecimiento anual promedio del 90%, lo que llevaría al mercado un valor de aproximadamente 2 mil millones de dólares para el año 2003.

De acuerdo con el modelo de ASP que propone Progress Software, cuando se vende la aplicación, le entrega al cliente la licencia que le permite operar, sobre los beneficios, no necesita comprar el software, ni realizar las tareas de implementación, a más de desligarse del hardware o de la plataforma en la cual va a operar. Trabajar bajo el modelo ASP de todas esas cuestiones tiene una clara ventaja: *sólo se paga por el uso*, de esta manera la empresa que contrata la modalidad puede orientar sus recursos humanos y financieros en base a sus necesidades y razón de ser de su negocio. El ASP ofrece la ventaja de no bloquear recursos humanos y financieros, que son muy escasos en América Latina.

1.2.- CARACTERÍSTICAS Y VENTAJAS QUE BRINDA UN ASP

En los siguientes listados se encuentran las características y ventajas más relevantes de un ASP.

1.2.1.- CARACTERÍSTICAS DE UN ASP

Un ASP dispone de características especiales de Hardware y Software que permita brindar total disponibilidad a los usuarios.

- El ASP posee y opera un software
- El ASP posee su propio servicio de Hosting donde ejecuta la aplicación
- El ASP también provee un servicio de mantenimiento continúo de la aplicación
- El ASP pone la aplicación a disposición de los clientes a través de Internet, mediante un navegador Web (Browser)
- El ASP cobra el uso de la aplicación por uso o sobre una base de cargos mensuales/anual

1.2.2.- VENTAJAS DE UN ASP

El modelo ASP ha evolucionado porque ofrece algunas ventajas significativas sobre modelos tradicionales. Aquí están algunas de las ventajas más importantes:

- Bajo costo de entrada y, en la mayoría de los casos, de un tiempo extremadamente corto de la puesta en marcha, en especial para las pequeñas empresas (pymes), como una de las mayores ventajas
- El modelo pago por uso es a menudo menos costoso
- El modelo del ASP también elimina la infraestructura especializada para la aplicación principal
- Aplicaciones listas para usarse
- La accesibilidad, conectividad y conveniencia de Internet

- Con el esquema de pago por uso, empresas de todo tamaño pueden ahora tener acceso a la tecnología de clase mundial, que antes sólo podían permitirse empresas con una actividad intensa de crédito
- Centralización de los datos
- Comunicación con sedes o departamentos remotos
- Ventajas del correo electrónico
- Publicidad de su marca o entidad
- Permite el acceso a plataformas que, por lo general, son caras y sólo están disponibles para las corporaciones
- Servicios a clientes
- Mayor velocidad de implementación
- Menores costos
- Posibilidades de E-Business
- Posibilidades de E-Commerce
- Información disponible 24x7 a través de Internet
- Respaldo y soporte técnico
- Seguridad, privacidad y confiabilidad

1.3.- COSTOS

Los clientes de los ASP pueden rentar los servicios por número de usuarios, por transacciones o por cuotas mensuales, este último esquema cubre en algunos casos el hardware, las licencias de software y la infraestructura de red en la cual correrán las aplicaciones, todo lo cual normalmente es posesión del ASP. La cuota también incluye el personal técnico de soporte para administrar y mantener los sistemas con un acuerdo contractual de nivel de servicio. Los clientes pueden optar también por rentar o comprar la aplicación. Algunas cuotas mensuales pueden variar desde cientos, hasta miles de dólares. Las rentas típicamente se acuerdan de 1 a 5 años.

En la siguiente tabla se presentan los costos estimados en un periodo de 3 años en un artículo publicado por aspnews.com, los costos son en dólares.

TABLA I-1 RELACIÓN DE COSTOS DE LOS SERVICIOS DE UN ASP PARA CONTRATAR UNA SOLUCIÓN ERP MEDIANTE OUTSOURCING

PRESUPUESTO	COSTOS INTERNOS 1ER AÑO	COSTOS INTERNOS 2DO AÑO	COSTOS INTERNOS 3ER AÑO	OUTSOURCING DURANTE POR LOS 3 AÑOS
Hardware (servidor de BD y servidor de aplicaciones)	70,000	20,000	20,000	Incluido
Software (Licencias para un ERP de 9 módulos)	800,000	200,000	500,000	incluido
Personal (DBAs y personal técnico)	265,000	265,000	265,000	incluido
Total Anual	1,135,000	485,000	785,000	900,000

Total en los 3 años			**$2,405,000**	
Costo promedio mensual	66,800	66,800	66,800	25,000

La tabla anterior es un ejemplo de una pequeña manufacturera norteamericana, quien al optar por contratar los servicios de un ASP para un ERP para 50 usuarios, en donde la personalización e implementación tomo 16 semanas

Algunas Preguntas y Respuestas para aclarar el panorama.

A continuación se presentan algunas preguntas con sus respectivas respuestas las mismas que van a permiten agrandar nuestro conocimiento de los ASP.

¿Que tipo de aplicaciones se pueden contratar?

Casi cualquier tipo de aplicación. La tecnología de compañías como Citrix, GraphOn y SCO que permiten a las aplicaciones que sean corridas en el ambiente de un ASP. La única diferencia es que la aplicación está corriendo en forma remota en un servidor central de Internet, ASP en lugar de estar en la propia empresa, muchas de las veces se debe realizar un estudio de la aplicación, puesto que si esta funciona de manera exitosa en el modelo tradicional talvez no lo hará de la misma manera al volcarlo en el modelo, por lo que habrá que rediseñarla.

¿Una aplicación que se corre en un ASP es en aspecto diferente a como se ve en la propia empresa?

La aplicación se ve del mismo modo que si estuviera en la empresa y funciona del mismo modo.

¿Puede obtener una solución personalizada?

Cada aplicación es personalizada de acuerdo a los requerimientos del cliente y luego hosteada solo para esa empresa. La flexibilidad que debe tener una aplicación ASP permite configurar en un tiempo record cada uno de los requerimientos del cliente.

1.4.- ¿QUÉ SERVICIOS OFRECE UN ASP?

Un ASP debe proveer servicios de alta calidad, que le van permitir ser preferido por varios cliente, caso contrario bueno el cliente se ira a otro ASP y habremos perdido esa cuenta.

1.4.1.- UN ASP TIENE QUE OFRECER LOS SIGUIENTES SERVICIOS

Como su nombre lo indica Proveedor de Servicio de Aplicación una de las partes más importantes son los servicio que brinda un ASP, en la siguiente lista se presentan algunos criterios que se debe tener en consideración al implementar un ASP.

- Escalabilidad y disponibilidad

- Facilidad de desarrollo y distribución

– Gestión de las aplicaciones

– Integración

– Inteligencia empresarial

1.4.1.1.- ESCALABILIDAD Y DISPONIBILIDAD

Cada vez son más las empresas que se deciden por este tipo de servicios, en un mercado creciente como es el de los ASP. La primera consecuencia que se puede obtener de este continuo crecimiento es que se pueden encontrar proveedores que no estén preparados para soportar una carga masiva de usuarios.

Y no sólo el software, sino también el hardware pueden provocar un cuello de botella en el caso de múltiples usuarios accediendo al sistema. Por ejemplo, las líneas de comunicaciones, la capacidad de proceso de los servidores o las aplicaciones encargadas de la seguridad pueden ralentizar el sistema, en tanto en cuanto el número de usuarios sea relativamente alto, las soluciones a estos problemas son múltiples, y dependen siempre de estudios estadísticos que estimen la tasa de crecimiento del proveedor, las necesidades de los usuarios, la capacidad de servicio que se desee ofrecer, etc. Como ya se ha comentado, una solución ASP no sólo por mejorar la capacidad del software, sino que también permite utilizar el software adecuado a cada situación.

Instalación del SO adecuado

- Aplicaciones que ofrecen seguridad deben ofrecer un servicio eficiente
- Seguridad física debe ser transparente al usuario (ej: backups realizados en períodos de baja actividad) .

- Capacidad de proceso de los servidores, y número de éstos .
- SGBD (Sistemas de Gestión de Bases de Datos) adecuados a cada aplicación
- Capacidad de las comunicaciones (infraestructura de red, entre otros).

Operatividad

Del mismo modo, no debería ser aceptable un servicio en el que las caídas del sistema son constantes, sino que sería deseable un 24 X 7, todo esto sin olvidar que el proveedor debe ofrecer una garantía de disponibilidad, relacionada con la seguridad, como por ejemplo ataques de crackers, virus, etc., que pueden afectar de una manera importante al servicio que se puede ofrecer, y que depende de la política del proveedor del servicio.

1.4.1.2.- FACILIDAD DE DESARROLLO Y DISTRIBUCIÓN

Relacionada con la anterior característica se encuentra la de la facilidad de desarrollo y distribución, que se refiere al proceso de actualizaciones que el proveedor puede ofrecer a la empresa.

Bien sabido es que la actualización de las aplicaciones es transparente al usuario que las utiliza, pero es importante tener en cuenta que dichas actualizaciones deben adaptarse en la medida de lo posible a las exigencias que nuestra empresa puede requerir y, por otro lado, que éstas no supongan un problema a la hora de “subir” de versión.

Una mala actualización de una aplicación, o una deficiencia a la hora de realizar una correcta batería de pruebas de la misma puede suponer un “parón” que redunda de nuevo en la disponibilidad del sistema. Por otro lado, la integridad del sistema debe maximizarse para que los problemas sean solucionados lo más rápido posible disminuyendo el impacto que los mismos pueden provocar

1.4.1.3.- GESTIÓN DE LAS APLICACIONES

Otro aspecto clave a tener en cuenta es el de la gestión de las aplicaciones. Si tenemos en cuenta que un proveedor de servicios de aplicaciones puede albergar en sus sistemas multitud de aplicaciones dirigidas a distintos tipos de usuarios, es importante que se lleve a cabo una buena gestión de configuración.

Por gestión de configuración entendemos la correcta gestión de las aplicaciones que componen el sistema, incluyendo información acerca de subidas de versión, cambios relevantes realizados tanto en el hardware como en el software, actualizaciones, y todo tipo de información que permita dejar “pistas” de auditoria.

Como decimos, la auditoria es un aspecto clave que diferencia a los proveedores. Y no sólo la externa, sino la interna es un tipo de auditoria que se basa en la investigación dentro de los límites del propio proveedor, y que busca aspectos que pueden ser mejorados, o criterios que pueden ser modificados en base a las necesidades de las empresas para ofrecer un mejor servicio.

Así mismo se pueden incluir en este grupo todo tipo de planes que ayuden a una mejor gestión de los sistemas del proveedor, tales como planes de contingencia y seguridad, planes de crecimiento basados en informes estadísticos y sobre viabilidad de proyectos, entre otros.

1.4.1.4.- INTEGRACIÓN

La integración se puede entender a dos niveles, interna y externa.

Integración interna:

Hace referencia al propio proveedor, es decir, a como es capaz de mezclar todos los componentes básicos para ofrecer a la empresa un sistema fiable, eficaz y eficiente. Un motor funciona bien si todos sus componentes funcionan bien, están bien integrados en el mismo y sus engranajes están bien engrasados.

Integración externa:

Hace referencia a la propia empresa que ha contratado los servicios del proveedor. Cuando se habla de integración externa nos referimos a la coordinación con las aplicaciones internas de la empresa, su propia infraestructura, su Software, entre otras. Para entendernos, si un proveedor permite un cierto tipo de flexibilidad y parametrización con los sistemas de la empresa de los servicios que ofrece, será más amigable que uno que ofrece un servicio rígido e independiente.

1.4.1.5.- INTELIGENCIA EMPRESARIAL

La inteligencia empresarial, también conocida como bussiness intelligence (BI), es un aspecto que está teniendo bastante auge en los últimos años. Suele venir unida al CRM (Customer Relationship Management), o técnicas de cuidado de clientes.

Se basa en la posibilidad de ofrecer servicios de valor añadido, basándose en distintas técnicas que permiten abordar la información de un modo más dinámico y menos rígido. Una de estas técnicas, aunque no la única, es la minería de datos o data minning, o la posibilidad de navegar por la información de un modo más parecido a como lo realizamos en la realidad (data marts), como por ejemplo obtener los distribuidores por productos y zonas, como decimos, el data minning es una técnica que permite obtener información relevante que no se encuentra de manera explicita en una sola base de datos, aplicando técnicas de inteligencia artificial, este es un aspecto que puede interesar a una empresa que está buscando un proveedor de servicios de aplicaciones, ya que ofrece un servicio de valor añadido. Por ejemplo,

a una empresa que ha contratado un servicio de una aplicación de distribución le puede interesar como añadido que se le informe de qué clientes son los más rentables, que le haga una previsión de crecimiento o que le informe de que clientes son candidatos a una potencial campaña publicitaria.

1.5.- ASPECTOS A CONSIDERAR EN LA CONTRATACIÓN DE LOS ASP

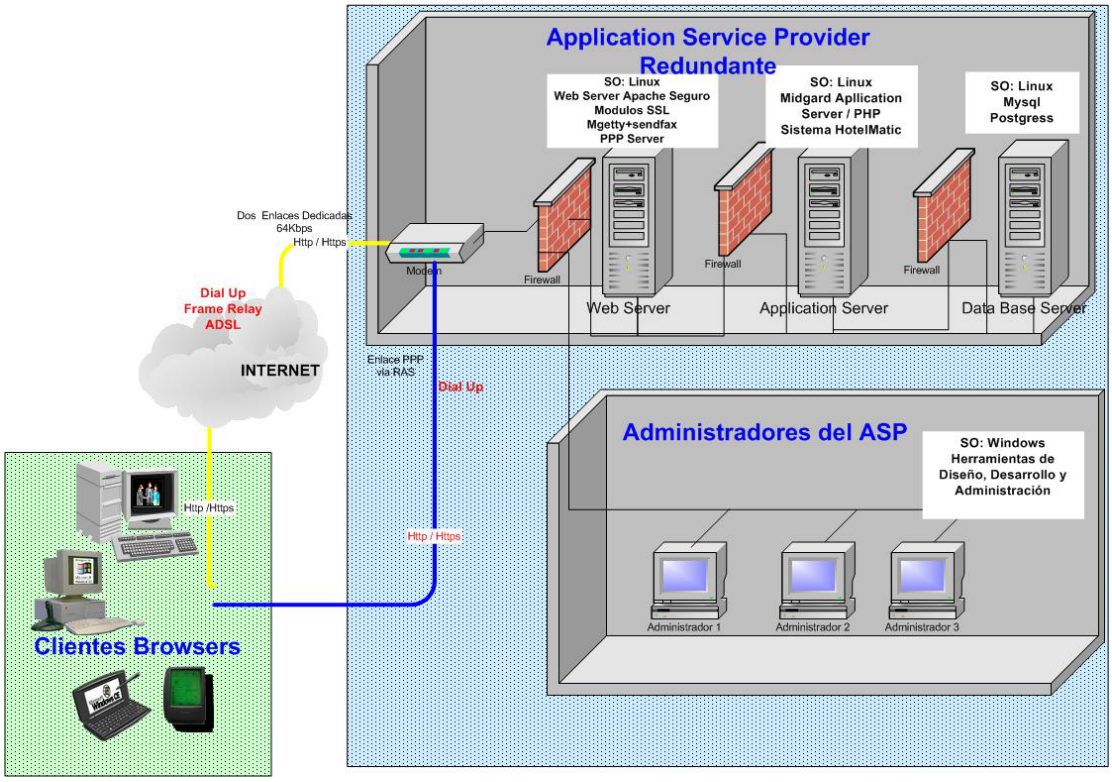
Dentro de los diferentes aspectos a tomar en cuenta en la selección de un ASP se encuentran los siguientes:

- Acceso al software ya sea a través de un navegador o de una aplicación
- Experiencias de otros clientes
- Soporte ofrecido
- Horario de atención
- Seguridad de los datos
- Seguridad de la conexión
- Mecanismos de contingencia y redundancia en caso de fallas
- Compartición de servidores y recursos con otros usuarios
- Planes para casos de emergencias o desastres
- Marco legal
- Formas de pago y contratación
- Formas de migrar la información en caso de optar por otro ASP

1.6.- DEFINICIÓN DE LA ARQUITECTURA ASP

En la siguiente imagen se presenta la arquitectura básica de un ASP y la interacción con los administradores y clientes.

FIGURA I-1 ARQUITECTURA BÁSICA DE UN ASP Y LA RELACIÓN CON SUS CLIENTES



1.6.1.- HARDWARE

A continuación daremos un breve vistazo sobre las características más importantes tomadas en cuenta para elegir los dispositivos de Hardware para la implantación de un ASP.

1.6.1.1.- SERVIDOR

Las características del equipo Servidor deben ser tales que se pueda respaldar la información del disco duro en otro, que soporte la atención de un alto número de usuarios, que sea estable bajo el sistema operativo elegido y compatible con el

hardware, la decisión por el Pentium III Dual pues la marca nos da la garantía del procesador y sus componentes además de recomendaciones de expertos.

1.6.1.2.- ESTACIONES DE DESARROLLO

El valor de un equipo Pentium es alto en comparación a un Athlon pero por las características del proyecto y las mejoras multimediales de los procesadores de AMD nos decidimos por el Athlon 900 Mhz(comparable con el Pentium de 750 Mhz), además de incorporarle a la placa madre una Tarjeta de video con especificaciones de memoria de video de 32 M y así poder aprovechar y mejorar la eficiencia de los programas que vamos a utilizar.

1.6.2.- SOFTWARE

De la misma manera como hemos visto los componentes de Harware veremos los componentes de Software más importantes.

1.6.2.1.- SISTEMA OPERATIVO PARA EL SERVIDOR

Linux Red Hat es un Sistema Operativo Freeware es decir gratuito, Linux Red Hat además proporciona el código fuente de la mayoría de sus aplicaciones haciendo que los administradores puedan revisar el código para detectar puertas traseras o algunos bugs que los programadores dejaron, esta es una característica que otros sistemas operativos tales como Windows no proveen que dejan a los servidores a merced de un acuerdo de licencia que se debe contestar satisfactoriamente si desea utilizar Windows como sistema operativo.

1.6.2.2.- SISTEMA OPERATIVO PARA ESTACIONES DE DESARROLLO Y/O ADMINISTRACIÓN

Frente a este punto no se tiene otra opción que equipar los computadores con alguna versión del sistema operativo windows (95/98/2000). Esto se debe a que muchas de las herramientas que necesitaremos, tales como: editores de imágenes, editores de video, editores de animación, no tienen sus versiones para Linux, que podría ser la otra alternativa. Luego, nuestra elección para optimizar el rendimiento de los equipos de desarrollo debe ser WINDOWS2000.

1.6.2.3.- WEB SERVER

Apache es el Web Server más utilizado en el mundo, además es gratuito según www.netcraft.com empresa dedicada al monitoreo de Internet en el mes de Marzo del 2002 mas del 53.76% de los servidores de Internet del mundo utilizaban a Apache como su Web Server, con esta premisa nos podemos dar cuenta de la potencia de Apache y de la aceptación por los expertos mundiales.

1.6.2.4.- APPLICATION SERVER

Hemos escogido como nuestro servidor de aplicaciones a Midgard por se al igual que Apache gratuito de las características que más nos llamo la atención es que está escrito en PHP al igual de tener total disponibilidad para trabajar con paginas dinámicas y Mysql que es la base de datos que hemos escogido, una de las desventajas es que no existe mucha información disponible en Internet de cómo usar Midgard.

1.6.2.5.- DATA BASE SERVER

Como Base de Datos hemos escogido a Mysql, su principal objetivo de diseño fue la VELOCIDAD. Se Sacrificaron algunas características esenciales en sistemas más “serios” con este fin otra característica importante es que consume muy pocos recursos, tanto de CPU como de memoria además de proveer licencia GLP a partir de la Versión 3.23.19 mediante la cual MYSQL.com entrega a su producto Mysql como binario y también su código fuente con el cual podemos adaptarla a nuestras necesidades.

1.6.2.6.- PHP LENGUAJE DE PROGRAMACIÓN

PHP es un lenguaje de programación orientado al Web permite realizar aplicaciones, tiene gran conectividad con la mayoría de las bases de datos comerciales o Freeware, ya sea utilizando drivers nativos o vía ODBC, de igual manera que Apache PHP es muy maduro ya se encuentra en la etapa de producción desde hace mucho tiempo atrás, según NetCarft a PHP se lo encuentra aproximadamente 5 millones de Dominios y su tasa de crecimiento es del 15% al mes.

La hipótesis de esta tesis es Implantar un ASP a bajo costo razón por la cual, buscamos herramientas de implementación y desarrollo que sean gratuitas es decir que estén bajo el paradigma GNU, GLP o de dominio público, el que sean gratuitas no quiere decir que sean malas o que estén llenas de bugs o puertas traseras, una anécdota de Unix fue que cuando se hicieron pruebas a sus Sistemas Operativos el que estaba siendo comercializado tenia muchos mas bugs que el que era entregado gratuitamente.

1.6.2.7.- UNIDADES DE RESPALDO DE INFORMACIÓN

Es muy importante el respaldo de información para lo cual una decisión acertada es la de grabar y respaldar en unidades de Cd la información y documentación del ASP

pero no descartamos la opción de la zip para el transporte de la información, pues se puede conectar a cualquier computador que tenga un puerto serial y es reconocida por Sistemas Operativos Windows.

Los requisitos de Hardware y Software de la siguiente tabla nos sirven como una base de referencia para poder implementar y permitir un buen desempeño de un ASP, con esto no queremos decir que esta es la Configuración Optima de un ASP, pero si es una de las más acertadas en el contexto que nos desarrollamos.

TABLA I-2 COMPONENTES DE HARDWARE Y SOFTWARE UTILIZADOS PARA LA IMPLANTACIÓN DEL ASP [1]

Recurso	Modelo	Cantidad	Precio c/u en usd	Precio total usd
Hardware				
Servidor	PIII- DUAL	2	$1.500.00	$3.000.00
PC Administración y Desarrollo y firewall	Athlon 900	4	$450.00	$1800.00
Hubs	Hub 3COM 16 puertos 10/100	2	$179.00	$358.00
Impresora	Lexmark Z32 870	2	$82.00	$164.00
Respaldo	Unidad Zip 250MB	1	$169.00	$169.00
Respaldo 2	CD-RWriter HP 8250 Externo	1	$220.00	$220.00
Subtotal en Hardware				$5711.00
Software				
Sistema Operativo	Red Hat 7.2	1	$0	$0

[1] Los Precios que se encuentran en esta lista están expuestos a cambios fecha 2002-04-01

Servidor	Red Hat 7.2	1	$0	$0
Firewall	Red Hat 7.2	1	$0	$0
SSL	Red Hat 7.2	1	$0	$0
Mgetty+sendfax	Mgetty	1	$0	$0
PPP	PPP-2.3.3	1	$0	$0
Base de Datos	Mysql	1	$0	$0
Lenguaje de Programación	PHP 4	1	$0	$0
Web Server	Apache	1	$0	$0
Application Server	Midgard 1.4	1	$0	$0
WS desarrollo	Windows98	3	$78.96	$236.88
PCs	Office Millenium	1	$102.72	$102.72
Certificado de Autentificación	VeriSing	*	*	*[2]
Web Mail	Squirrelmail	1	$0	$0
Subtotal en Software				$339.6
Desarrollo				
Editor Gráfico	Photoshop5.5	1	$411.60	$411.60
Editor HTML	Deamweaver Ultradev	1	$273.71	$273.71
Editor Animaciones	Flash 5.0	1	$273.71	$273.71
Lenguaje de Programación	PHP-4.0.6-WIN32	1	$0	$0
Base de Datos	mysql-3.23.39ª-win	1	$0	$0
Servidor Web apache para Windows	apache_1.3.22-win32-x86	1	$0	$0
Administrador DB	PhpMyAdmin	1	$0	$0
Editor de PHP	Phpcode	1	$0	$0
Subtotal en Desarrollo				$959.02

[2] Estos precios se deben de consultar el www.verisign.com puesto que existen muchos tipos de certificados, y cada uno tiene diferentes características de uso y presentación

Comunicaciones				
Salida a Internet Telconet	Enlace 64Kbps /Ilimitado	1	$750	$750
Salida a Internet Satnet	Enlace 64Kbps/Ilimitado	1		
Líneas Telefónicas	Enlace RAS	3	$300	$900
Subtotal en Comunicaciones				$1050
Total				**$8059.62**

1.7.- ESPECIFICACIONES TÉCNICAS DE UN ASP

El rendimiento del ASP depende de un número elevado de variables que debemos tener en consideración tales como:

- Número de Clientes que serán atendidos.
- Número de páginas estáticas (.html,.gif, .jpg) versus las páginas que serán generadas por los lenguajes de scripting.
- Complejidad de la codificación del Script
- Tamaño y diseño de la Base de Datos.
- Tener muy en cuenta si utilizaremos un motor de búsqueda
- Uso de encriptación tal como la tecnología SSL.
- Número de Aplicaciones Hosteadas en el Servidor.

Existen muchos más variables a tomar en cuenta para especificar la parte técnica de un ASP aquí propongo una configuración para 100 clientes concurrentes.

TABLA I-3 ESPECIFICACIONES DE HARDWARE PARA UN ASP CONSIDERADO PEQUEÑO

Configuración	Procesador	Nro de Procesadores	Memoria	Capacidad en Disco Duro
100 Clientes Concurrentes	Pentium III	1→2	512MB/1GB	30GB/40GB

TABLA I -4 ESPECIFICACIONES DE HARDWARE PARA UN ASP PARA LOS ADMINISTRADORES

Configuración	Procesador	Procesadores	Memoria	Capacidad en HD
1	Pentium III	1	128MB	20

Además de las Consideraciones de Hardware debemos de tener en cuenta las comunicaciones y la disponibilidad.

Para las comunicaciones utilizamos dos conexiones dedicadas con diferentes (ISP's), de esta manera estaremos cuidando la disponibilidad, ya que si un proveedor de Internet falla, los clientes del ASP pueden acceder a través del segundo proveedor de Internet y si éste llegase a fallar también, el ASP tiene a disposición un número suficiente de líneas telefónicas para que puedan acceder al servidor de aplicaciones mediante vía RAS (Remote Access Service).

Para mantener la disponibilidad del servicio el ASP utiliza un término conocido como Redundancia tanto en los servidores como en las comunicaciones, sola mente de esta manera se puede logran una disponibilidad 24*7, la Redundancia es un termino muy utilizado a nivel mundial se trata tener todo repetido ya sea 2 más veces.

1.8.- CASO DE ESTUDIO: DATADEC EMPRESA LÍDER COMO ASP

Datadec se constituyó en 1987 con el objetivo de desarrollar una solución de gestión empresarial que cubriera las necesidades de la mediana y gran empresa y con la visión de resolverlas de manera integrada y modular, tanto en un entorno de tecnología cliente/servidor como de navegador web para el mundo Internet.

1.8.1.- SOBRE SU INFRAESTRUCTURA

En el centro de datos de Datadec Online se ha diseñado e implantado una arquitectura de proceso para permitir el mayor nivel de disponibilidad y fiabilidad, que garantice las transacciones electrónicas de los clientes.

Por el nivel de seguridad y escalabilidad, la plataforma elegida está basada en modelos de Compaq.

Datadec Online utiliza sistemas Compaq Alpha Server con sistema operativo Tru64 Unix y Compaq Intel con sistema operativo Windows 2000, ambas plataformas están integradas en sistema clúster, lo que aumenta la potencia y el nivel de disponibilidad varios procesadores trabajando simultáneamente incrementan la escalabilidad del sistema en su conjunto, al mismo tiempo que la redundancia garantiza el servicio.

A nivel de protección lógica, los servidores están continuamente monitorizados y protegidos por cortafuegos. Además se utilizan sistemas de backup y restauración desatendidos y la arquitectura de almacenamiento radica en una SAN en Raid hot-plug.

1.8.2.- TECNOLOGÍA

DATADEC tiene una tecnología impresionante la cual la listamos a continuación

- Hardware: Plataforma Compaq Alpha Server redundante y plataforma Compaq Intel también redundante.
- Sistema operativo: Clúster Tru64 Unix y Clúster Windows 2000
- Bases de datos: Oracle 8, Parallel Server
- Servidor de aplicaciones: Oracle IAS 9i y Microsoft IIS
- Servidor de correo: Microsoft Exchange, Sendmail
- Cortafuegos: Checkpoint
- Antivirus: Trendmicro
- Balanceador de cargas: Redware
- Sistema de detección de intrusos: Real Secure
- Tráfico modo seguro: SSL

Como podemos ver luego de un vistazo breve por el Internet, los ASP en el mundo los tenemos de muchos colores y para todos los gustos, en el mundo existen muchos ASP con una Infraestructura Tecnológica muy Impresionante, esto depende de la cantidad de clientes a los que se desee atender y de la diversidad de aplicaciones hosteadas en los servidores, no nos olvidemos que una de las características que debemos cuidar es que los ASP se deben encontrar siempre a la vanguardia tecnológica puesto que de otra manera nuestros clientes se cambiaran de proveedor.

El Prototipo Operativo va a ser implantado en PC, además reunir a todas las características de un ASP y los estándares de seguridad que la organización allASP establece para ser considerado como ASP

Capitulo

2

II.- SEGURIDADES QUE DEBE OFRECER UN ASP

Una de las características más fundamentales de un ASP es el de proveer la aplicación utilizando Internet o un red privada virtual, lo que hace que sea un blanco fácil para que personas inescrupulosas o curiosas pretendan apoderarse de lo que no es suyo o simplemente eliminar la información, en este capítulo veremos algunos de los criterios de seguridad no solo en el Hardware , Software o red sino también en algo que muchos de los administradores de los centros de datos se olvidan como son las seguridades físicas, el objetivo final de este capitulo es marcar unas pautas para conseguir un nivel de seguridad aceptable en los sistemas conectados en cualquier red.

2.1.- SEGURIDADES EN INTERNET

Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadores de propósito general. Mientras que por una parte Internet iba creciendo exponencialmente con redes importantes que se adherían a ella, como BITNET o HEPNET, por otra el auge de la informática de consumo (hasta la década de los ochenta muy poca gente se podía permitir un ordenador y un módem en casa) unido a factores menos técnicos (como la película Juegos de Guerra, de 1983) iba produciendo un aumento espectacular en el número de piratas informáticos.

Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso worm o gusano de Internet. Miles de ordenadores conectados a la red

se vieron inutilizados durante días, y las pérdidas se estiman en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. Poco después de este incidente, y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos estadounidenses (en general, a los sistemas de cualquier país) la agencia DARPA (Defense Advanced Research Projects Agency) creó el CERT (Computer Emergency Response Team), un grupo formado en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten a hosts de Internet .

Han pasado más de diez años desde la creación del primer CERT, y cada día se hace patente la preocupación por los temas relativos a la seguridad en la red y sus equipos y también se hace apremiante la necesidad de esta seguridad. Los piratas de antaño casi han desaparecido dando paso a nuevas generaciones de intrusos que forman grupos como Chaos Computer Club o Legion of Doom, organizan encuentros como el español Iberhack, y editan revistas o zines electrónicos (2600: The Hacker's Quartely o Phrack son quizás las más conocidas, pero no las únicas). Todo esto con un objetivo principal compartir conocimientos, si hace unos años cualquiera que quisiera adentrarse en el mundo underground casi no tenía más remedio que conectar a alguna BBS donde se tratara el tema, generalmente con una cantidad de información muy limitada, hoy en día tiene a su disposición gigabytes de información electrónica publicada en Internet cualquier aprendiz de pirata puede conectarse a un servidor Web descargar un par de programas y ejecutarlos contra un servidor desprotegido, con un poco de mala suerte esa misma persona puede conseguir un control total sobre un servidor Unix de varios millones de dólares, probablemente desde su PC con Windows 98 y sin saber nada sobre Unix. De la misma forma que en su día Juegos de Guerra creó una nueva generación de piratas, en la segunda mitad de los noventa películas como The Net, Hackers o Los Corsarios del Chip han creado otra generación, en general mucho menos peligrosa que la anterior, pero cuanto

menos, preocupante aunque sin grandes conocimientos técnicos, tienen a su disposición multitud de programas y documentos sobre seguridad algo que los piratas de los ochenta apenas podían imaginar, además de ordenadores potentes y conexiones a Internet baratas. Por si esto fuera poco, se ven envalentonados a través de sistemas de conversación como el IRC (Internet Relay Chat), donde en canales como hack o hackers presumen de sus logros ante sus colegas.

2.1.1.- JUSTIFICACIÓN Y OBJETIVOS

A la vista de lo comentado en el primer punto, parece claro que la seguridad de los equipos ha de ser algo a considerar en cualquier red, diariamente por cualquiera de ellas circulan todo tipo de datos, entre ellos muchos que se podrían catalogar como confidenciales (nóminas, expedientes, presupuestos) o al menos como privados (correo electrónico, proyectos de investigación, artículos a punto de ser publicados). Independientemente de la etiqueta que cada usuario de la red quiera colgarle a sus datos, parece claro que un fallo de seguridad de un equipo o de la propia red no beneficia a nadie, y mucho menos a la imagen de nuestra organización, ya no se trata simplemente de una cuestión de imagen según el Computer Security Institute, en su encuesta de 1998, las pérdidas económicas ocasionadas por delitos relacionados con nuevas tecnologías (principalmente accesos internos no autorizados) sólo en Estados Unidos ascienden anualmente a más 20.000 millones de dólares, cifra que cada año se incrementa en más del 35%; los delitos informáticos en general aumentan también de forma espectacular año tras año, alcanzando incluso cotas del 800%.

El objetivo final de este capitulo es marcar unas pautas para conseguir un nivel de seguridad aceptable en los sistemas conectados en cualquier red, entendiendo por ‘aceptable' un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los equipos de nuestra organización fracasara ante un ataque contra los mismos. Obviamente, es imposible garantizar una plena seguridad ante cualquier atacante seguramente un pirata experimentado, con el tiempo suficiente, pagado, o simplemente muy interesado en uno de nuestros

equipos, no tendría muchos problemas en acceder a él, este hecho aunque preocupante es casi inevitable lo evitable es que cualquier persona sea capaz de atacar con éxito un equipo simplemente por haber visto una película descargado un par de páginas Web y ejecutado un programa que ni ha hecho ni entiende.

2.1.2.- QUÉ ES SEGURIDAD?

Podemos entender como seguridad una característica de cualquier sistema informático o no que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es en cierta manera infalible. Como esta característica particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir, según la mayoría de expertos imposible se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: *confidencialidad, integridad y disponibilidad.*

Qué implica cada uno de los tres aspectos de los que hablamos? La *confidencialidad* nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad: un sistema Linux puede conseguir confidencialidad para un determinado fichero haciendo que ningún usuario ni siquiera el root pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad seguramente es preferible que alguien borre información confidencial que se podría recuperar después desde una cinta de backup a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados, en cambio en un servidor NFS de un departamento se premiará la disponibilidad frente a la confidencialidad importa poco que un atacante lea una unidad, pero que esa misma unidad no sea leída por usuarios autorizados va a suponer una pérdida de tiempo y dinero. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

2.1.3.- QUÉ QUEREMOS PROTEGER?

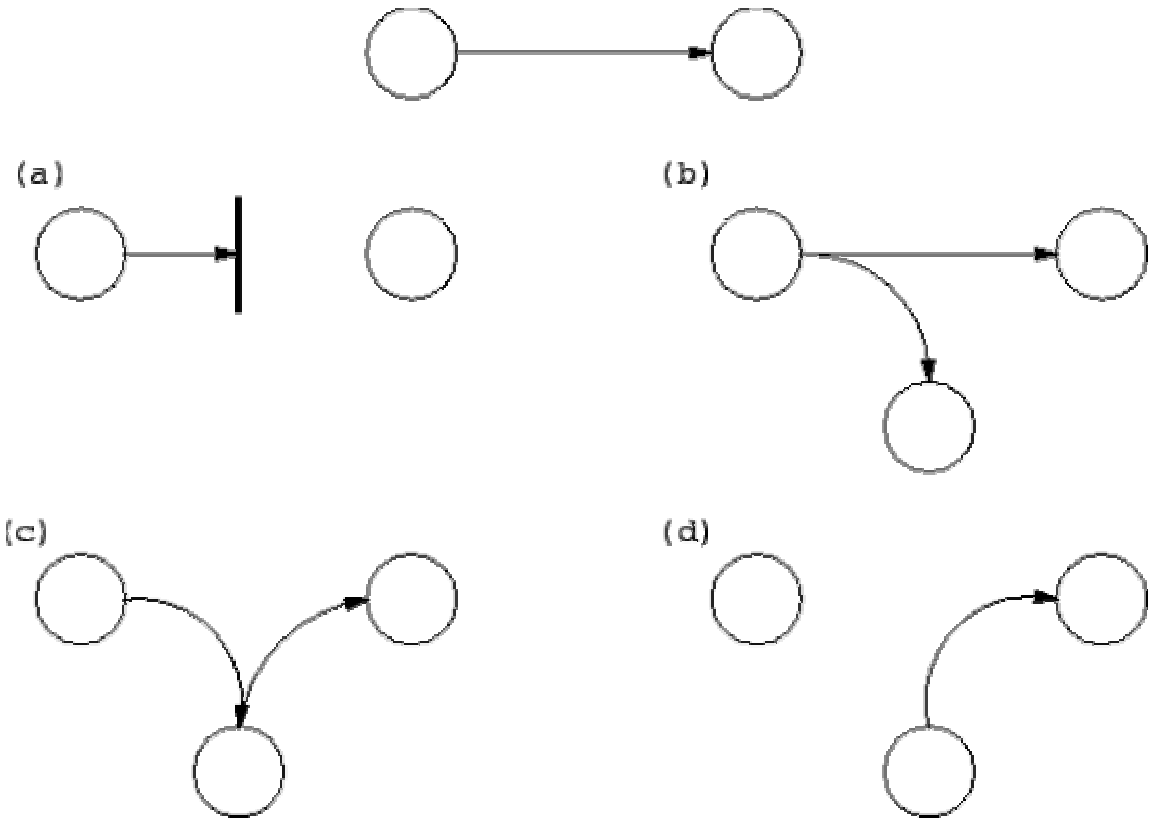
Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, disquetes, entre otros) o tarjetas de red. Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones y por datos el conjunto de información lógica que manejan el software y el hardware, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorias de seguridad se habla de un cuarto elemento a proteger, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, tóners, cintas magnéticas, disquetes), aquí no consideraremos la seguridad de estos elementos por ser externos al sistema.

Habitualmente los datos constituyen el principal elemento de los tres a proteger ya que es el más amenazado y seguramente el más difícil de recuperar con toda seguridad una máquina está ubicada en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación o un programa de sistema o el propio núcleo de Linux este software se puede restaurar sin problemas desde su medio original (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación), sin embargo en caso de pérdida de una base de datos o de un proyecto de un usuario no tenemos un medio original desde el que restaurar hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

Contra cualquiera de los tres elementos descritos anteriormente pero principalmente sobre los datos se pueden realizar multitud de ataques o dicho de otra forma están expuestos a diferentes amenazas, generalmente la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto, algunos autores consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado, por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado.

En la siguiente figura se muestran estos tipos de ataque de una forma gráfica.

FIGURA II-0-1 FLUJO NORMAL DE INFORMACIÓN ENTRE EMISOR Y RECEPTOR Y POSIBLES AMENAZAS: (A) INTERRUPCIÓN, (B) INTERCEPTACIÓN, (C) MODIFICACIÓN Y (D) FABRICACIÓN



2.2.- SEGURIDADES FÍSICAS EN UN ASP

La seguridad física de los sistemas informáticos preferentemente de un ASP consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial. Más claramente, y particularizando para el caso de equipos Linux y sus centros de operación, por seguridad física podemos entender todas aquellas mecanismos generalmente de prevención y detección destinados

a proteger físicamente cualquier recurso del sistema, estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia a la hora de hablar de seguridad informática en general en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema, esto motiva que en determinadas situaciones un atacante se decline por aprovechar vulnerabilidades físicas en lugar de lógicas ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él mediante fallos en el software. Hemos de ser conscientes de que la seguridad física es demasiado importante como para ignorarla: un ladrón que roba un ordenador para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones nos pueden hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada no importa que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que hayamos definido una política de firewalling muy restrictiva si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada. Además en el caso de organismos con requerimientos de seguridad medios, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas como casi todos los atacantes de los equipos de estos entornos son casuales (esto es, no tienen interés específico sobre nuestros equipos, sino sobre cualquier equipo), si notan a través de medidas físicas que nuestra organización está preocupada por la seguridad probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida

No vamos a centrarnos en el diseño de edificios resistentes a un terremoto o en la instalación de alarmas electrónicas, sí que se van a intentar comentar ciertas medidas de prevención y detección que se han de tener en cuenta a la hora de

definir mecanismos y políticas para la seguridad de nuestros equipos. Pero hemos de recordar que cada sitio es diferente, y por tanto también lo son sus necesidades de seguridad de esta forma no se pueden dar recomendaciones específicas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es el cerrar con llave la sala de operaciones cuando salimos de ella) hasta medidas mucho más complejas como la prevención de radiaciones electromagnéticas de los equipos. En entornos habituales suele ser suficiente con un poco de sentido común para conseguir una mínima seguridad física, de cualquier forma en cada institución se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado. Por ejemplo, en una empresa ubicada en Valencia quizás parezca absurdo hablar de la prevención ante terremotos (por ser esta un área de bajo riesgo), pero no sucederá lo mismo en una empresa situada en Los Ángeles que es una zona sísmica mente activa de la misma forma, en entornos de I+D es absurdo hablar de la prevención ante un ataque nuclear, pero en sistemas militares esta amenaza se ha de tener en cuenta.

2.2.1.- PROTECCIÓN DEL HARDWARE

El hardware es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización, especialmente en las dedicadas a I+D universidades, centros de investigación, institutos tecnológicos, entre otros suelen poseer alguno de sus equipos máquinas muy caras, desde servidores con una gran potencia de cálculo hasta routers de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica.

2.2.2.- ACCESO FÍSICO

La posibilidad de acceder físicamente a una máquina en general a cualquier sistema operativo hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre ella hemos de pensar que si un atacante puede llegar con total libertad hasta una estación puede por ejemplo abrir la CPU y llevarse un disco duro sin necesidad de privilegios en el sistema, sin importar la robustez de nuestros cortafuegos sin ni siquiera una clave de usuario, el atacante podrá seguramente modificar la información almacenada, destruirla o simplemente leerla. Incluso sin llegar al extremo de desmontar la máquina que quizás resulte algo exagerado en entornos clásicos donde hay cierta vigilancia como un laboratorio o una sala de informática, la persona que accede al equipo puede pararlo o arrancar una versión diferente del sistema operativo sin llamar mucho la atención. Si por ejemplo alguien accede a un laboratorio con máquinas Linux, seguramente le resultará fácil utilizar un disco de arranque, montar los discos duros de la máquina y extraer de ellos la información deseada incluso es posible que utilice un ramdisk con ciertas utilidades que constituyan una amenaza para otros equipos como nukes o sniffers.

Visto esto parece claro que cierta seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas conectados a ella evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger (no es necesario hablar sólo de equipos Linux, sino de cualquier elemento físico que se pueda utilizar para amenazar la seguridad, como una toma de red apartada en cualquier rincón de un edificio de nuestra organización). Mientras que parte de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento o las máquinas de los despachos, otros muchos estarán en lugares de acceso semipúblico, como laboratorios de prácticas es justamente sobre estos últimos sobre los que debemos extremar las precauciones ya que lo más fácil y discreto para un atacante es acceder a uno de estos equipos y en segundos lanzar un ataque completo sobre la red.

2.2.3.- PREVENCIÓN

Como se puede prevenir un acceso físico no autorizado a un determinado punto, hay soluciones para todos los gustos y también de todos los precios desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta. Todos los modelos de autenticación de usuarios son aplicables, aparte de para controlar el acceso lógico a los sistemas, para controlar el acceso físico de todos ellos, quizás los más adecuados a la seguridad física sean los biométricos y los basados en algo poseído, aunque como comentaremos más tarde suelen resultar algo caros para utilizarlos masivamente en entornos de seguridad media.

Pero no hay que irse a sistemas tan complejos para prevenir accesos físicos no autorizados normas tan elementales como cerrar las puertas con llave al salir de un laboratorio o un despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados son en ocasiones más que suficientes para prevenir ataques. También basta el sentido común para darse cuenta de que el cableado de red es un elemento importante para la seguridad, por lo que es recomendable apartarlo del acceso directo, por desgracia en muchas organizaciones podemos ver excelentes ejemplos de lo que no hay que hacer en este sentido cualquiera que pasee por entornos más o menos amplios (el campus de una universidad, por ejemplo) seguramente podrá ver, pinchar o cortar cables descolgados al alcance de todo el mundo, especialmente durante el periodo de vacaciones época que se suele aprovechar para hacer obras.

Todos hemos visto películas en las que se mostraba un estricto control de acceso a instalaciones militares mediante tarjetas inteligentes, analizadores de retina o verificadores de la geometría de la mano aunque algunos de estos métodos aún suenen a ciencia ficción y sean demasiado caros para la mayor parte de entornos (recordemos que si el sistema de protección es más caro que lo que se quiere proteger tenemos un grave error en nuestros planes de seguridad),

otros se pueden aplicar, y se aplican, en muchas organizaciones. Concretamente el uso de lectores de tarjetas para poder acceder a ciertas dependencias es algo muy a la orden del día la idea es sencilla, alguien pasa una tarjeta por el lector, que conecta con un sistema por ejemplo un ordenador en el que existe una base de datos con información de los usuarios y los recintos a los que se le permite el acceso. Si la tarjeta pertenece a un usuario capacitado para abrir la puerta, ésta se abre y en caso contrario se registra el intento y se niega el acceso, aunque este método quizás resulte algo caro para extenderlo a todos y cada uno de los puntos a proteger en una organización, no sería tan descabellado instalar pequeños lectores de códigos de barras conectados a una máquina en las puertas de muchas áreas, especialmente en las que se maneja información más o menos sensible. Estos lectores podrían leer una tarjeta que todos los miembros de la organización poseerían, conectar con la base de datos de usuarios y autorizar o denegar la apertura de la puerta. Se trataría de un sistema sencillo de implementar no muy caro y que cubre de sobra las necesidades de seguridad en la mayoría de entornos incluso se podría abaratar si en lugar de utilizar un mecanismo para abrir y cerrar puertas el sistema se limitara a informar al administrador del área o a un guardia de seguridad mediante un mensaje en pantalla o una luz encendida, de esta forma los únicos gastos serían los correspondientes a los lectores de códigos de barras ya que como equipo con la base de datos se puede utilizar una máquina vieja o un servidor de propósito general.

2.2.4.- DETECCIÓN

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano) es deseable que un potencial ataque sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la detección de problemas, generalmente accesos físicos no autorizados, intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, en entornos más normales el esfuerzo en detectar estas amenazas se ha de centrar en las personas que utilizan los sistemas y en las que sin utilizarlos están relacionadas de cierta forma con ellos

sucede lo mismo que con la seguridad lógica se ha de ver toda la protección como una cadena que falla si falla su eslabón más débil.

Es importante concienciar a todos de su papel en la política de seguridad del entorno si por ejemplo un usuario autorizado detecta presencia de alguien de quien sospecha que no tiene autorización para estar en una determinada estancia debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario. No obstante, utilizar este servicio debe ser solamente un último recurso: generalmente en la mayoría de entornos no estamos tratando con terroristas, sino por fortuna con elementos mucho menos peligrosos. Si cada vez que se sospecha de alguien se avisa al servicio de seguridad esto puede repercutir en el ambiente de trabajo de los usuarios autorizados estableciendo cierta presión que no es en absoluto recomendable, un simple puedo ayudarte en algo? suele ser más efectivo que un guardia solicitando una identificación formal. Esto es especialmente recomendable en lugares de acceso restringido, como laboratorios de investigación o centros de cálculo, donde los usuarios habituales suelen conocerse entre ellos y es fácil detectar personas ajenas al entorno.

2.2.5.- DESASTRES NATURALES

En el anterior punto hemos hecho referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física. Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su falta de prevención.

2.2.5.1.- TERREMOTOS

Los terremotos son el desastre natural muy probable en Ecuador, esta es una zona donde se suelan producir temblores de intensidad considerable de cualquier forma, aunque algunas medidas contra terremotos son excesivamente caras para la mayor parte de organizaciones en Ecuador evidentemente serían igual de caras en zonas como Los Ángeles, pero allí el coste estaría justificado por la alta probabilidad de que se produzcan movimientos de magnitud considerable, no cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar nunca equipos delicados en superficies muy elevadas aunque tampoco es bueno situarlos a ras de suelo, como veremos al hablar de inundaciones. Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo hardware, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente y barato utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los routers. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarán el hardware.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la pérdida de datos o hardware pierde importancia frente a los posibles accidentes incluso mortales que puede causar una pieza voluminosa a las personas a las que les cae encima. Además, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que se descuelgue por la fachada hasta las ventanas, ya que si el equipo estuviera cerca no tendría más que alargar el brazo para llevárselo.

No obstante, no debemos entender por terremotos únicamente a los grandes desastres que derrumban edificios y destrozan vías de comunicación, quizás sería más apropiado hablar incluso de vibraciones, desde las más grandes (los terremotos) hasta las más pequeñas (un simple motor cercano a los equipos). Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier

elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con hardware más mecánico, como las impresoras estos dispositivos no paran de generar vibraciones cuando están en funcionamiento por lo que situar una pequeña impresora encima de la CPU de una máquina es una idea nefasta. Como dicen algunos expertos en seguridad, el espacio en la sala de operaciones es un problema sin importancia comparado con las consecuencias de fallos en un disco duro o en la placa base de un ordenador.

2.2.5.2.- TORMENTAS ELÉCTRICAS

Las tormentas eléctricas son muy frecuentes en verano cuando mucho personal se encuentra de vacaciones, lo que las hace más peligrosas generan subidas súbitas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica, como veremos a continuación. Si cae un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir hardware incluso protegido contra voltajes elevados.

Sin embargo, las tormentas poseen un lado positivo: son predecibles con más o menos exactitud, lo que permite a un administrador parar sus máquinas y desconectarlas de la línea eléctrica. Entonces, ¿Cuál es el problema? Aparte de las propias tormentas, el problema son los responsables de los equipos: la caída de un rayo es algo poco probable pero no imposible en una gran ciudad donde existen artilugios destinados justamente a atraer rayos de una forma controlada

tanto es así que mucha gente ni siquiera ha visto caer cerca un rayo, por lo que directamente tiende a asumir que eso no le va a suceder nunca, y menos a sus equipos. Por tanto, muy pocos administradores se molestan en parar máquinas y desconectarlas ante una tormenta; si el fenómeno sucede durante las horas de trabajo y la tormenta es fuerte, quizás sí que lo hace, pero si sucede un sábado por la noche nadie va a ir a la sala de operaciones a proteger a los equipos, y nadie antes se habrá tomado la molestia de protegerlos por una simple previsión meteorológica. Si a esto añadimos lo que antes hemos comentado, que las tormentas se producen con más frecuencia en pleno verano, cuando casi toda la plantilla está de vacaciones y sólo hay un par de personas de guardia, tenemos el caldo de cultivo ideal para que una amenaza que a priori no es muy grave se convierta en el final de algunos de nuestros equipos. Conclusión, todos hemos de tomar más en serio a la Naturaleza cuando nos avisa con un par de truenos.

Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad deben ser almacenadas lo más alejados posible de la estructura metálica de los edificios un rayo en el propio edificio, o en un lugar cercano puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el hardware la pérdida de toda la información de nuestros sistemas.

2.2.5.3.- INUNDACIONES Y HUMEDAD

Cierto grado de humedad es necesario para un correcto funcionamiento de nuestras máquinas en ambientes extremadamente secos el nivel de electricidad estática es elevado, esto puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, en un daño irreparable al hardware y a la información. No obstante niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina.

Controlar el nivel de humedad en los entornos habituales es algo innecesario, ya que por norma nadie ubica estaciones en los lugares más húmedos o que presenten situaciones extremas no obstante, ciertos equipos son especialmente sensibles a la humedad por lo que es conveniente consultar los manuales de todos aquellos de los que tengamos dudas. Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o demasiada humedad, especialmente en sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

Cuando ya no se habla de una humedad más o menos elevada, sino de inundaciones completas, los problemas generados son mucho mayores. Casi cualquier medio (una máquina, una cinta, un router) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos.

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención frente a las de detección podemos utilizar detectores de agua en los suelos o falsos suelos de las salas de operaciones, y apagar automáticamente los sistemas en caso de que se activen. Tras apagar los sistemas podemos tener también instalado un sistema automático que corte la corriente: algo muy común es intentar sacar los equipos previamente apagados o no de una sala que se está empezando a inundar; esto, que a primera vista parece lo lógico, es el mayor error que se puede cometer si no hemos desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar equipos. Por muy caro que sea el hardware o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a lo que supone la pérdida de vidas humanas. Otro error común relacionado con los detectores de agua es situar a los mismos a un nivel superior que a los propios equipos a salvaguardar incluso en el techo, junto a los detectores de humo evidentemente, cuando en estos casos el agua llega al detector poco se puede hacer ya por las máquinas o la información que contienen.

Medidas de protección menos sofisticadas pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

2.2.6.- DESASTRES DEL ENTORNO

En las líneas siguientes se presenta los desastres más comunes, además de presentar las formas más fáciles de evitarlos.

2.2.6.1.- ELECTRICIDAD

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como picos porque generalmente duran muy poco durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al hardware o a los datos gracias a que en la mayoría de equipos hay instalados fusibles, elementos que se funden ante una subida de tensión y dejan de conducir la corriente, provocando que la máquina permanezca apagada. Disponga o no de fusibles el equipo a proteger lo normal es que sí los tenga una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad estos mecanismos evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo de una sala o edificio, o simplemente hacia cualquier lugar con voltaje nulo. Una toma de tierra sencilla

puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se introduce lo más posible en el suelo; el coste de la instalación es pequeño, especialmente si lo comparamos con las pérdidas que supondría un incendio que afecte a todos o a una parte de nuestros equipos.

Incluso teniendo un sistema protegido con los métodos anteriores, si la subida de tensión dura demasiado, o si es demasiado rápida, podemos sufrir daños en los equipos; existen acondicionadores de tensión comerciales que protegen de los picos hasta en los casos más extremos, y que también se utilizan como filtros para ruido eléctrico. Aunque en la mayoría de situaciones no es necesario su uso, si nuestra organización tiene problemas por el voltaje excesivo quizás sea conveniente instalar alguno de estos aparatos.

Un problema que los estabilizadores de tensión o las tomas de tierra no pueden solucionar es justamente el contrario a las subidas de tensión: las bajadas, situaciones en las que la corriente desciende por debajo del voltaje necesario para un correcto funcionamiento del sistema, pero sin llegar a ser lo suficientemente bajo para que la máquina se apague. En estas situaciones la máquina se va a comportar de forma extraña e incorrecta, por ejemplo no aceptando algunas instrucciones, no completando escrituras en disco o memoria, etc. Es una situación similar a la de una bombilla que pierde intensidad momentáneamente por falta de corriente, pero trasladada a un sistema que en ese pequeño intervalo ejecuta miles o millones de instrucciones y transferencias de datos.

Otro problema, muchísimo más habitual que los anteriores en redes eléctricas modernas, son los cortes en el fluido eléctrico que llega a nuestros equipos. Aunque un simple corte de corriente no suele afectar al hardware, lo más peligroso y que sucede en muchas ocasiones son las idas y venidas rápidas de la corriente en esta situación, aparte de perder datos, nuestras máquinas pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar una SAI (Servicio de Alimentación Ininterrumpido) conectada al elemento que queremos proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable de corriente, protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen capacidad para seguir alimentando las máquinas incluso en caso de que no reciban electricidad evidentemente no las alimentan de forma indefinida, sino durante un cierto tiempo el necesario para detener el sistema de forma ordenada. Por tanto, en caso de fallo de la corriente el SAI informará a la máquina Linux, que a través de un programa como /sbin/powerd recibe la información y decide cuanto tiempo de corriente le queda para poder pararse correctamente; si de nuevo vuelve el flujo la SAI vuelve a informar de este evento y el sistema desprograma su parada. Así de simple por poco más de 500 dólares podemos obtener una SAI pequeña, más que suficiente para muchos servidores que nos va a librar de la mayoría de los problemas relacionados con la red eléctrica.

Un último problema contra el que ni siquiera las SAIs nos protegen es la corriente estática, un fenómeno extraño del que la mayoría de gente piensa que no afecta a los equipos, sólo a otras personas. Nada más lejos de la realidad simplemente tocar con la mano la parte metálica de teclado o un conductor de una placa puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño sólo un pequeño calambrazo el ordenador sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM. Contra el problema de la corriente estática existen muchas y muy baratas soluciones: spray antiestático, ionizadores antiestáticos, no obstante en la mayoría de situaciones sólo hace falta un poco de sentido común del usuario para evitar accidentes: no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el hardware, no mantener el entorno excesivamente seco.

2.2.6.2.- RUIDO ELÉCTRICO

Este problema no es una incidencia directa de la corriente en nuestros equipos, sino una incidencia relacionada con la corriente de otras máquinas que pueden afectar al funcionamiento de la nuestra. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar no situar hardware cercano a la maquinaria que puede causar dicho ruido; si no tenemos más remedio que hacerlo, podemos instalar filtros en las líneas de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies estos elementos puede incluso dañar permanentemente a nuestro hardware si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

2.2.6.3.- INCENDIOS Y HUMO

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo aunque la causa de un fuego puede ser un desastre natural lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio, o al menos en la planta, donde se encuentran invertidos miles de dólares en equipamiento.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los

más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el hardware no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero que quedara destrozado por el agua expulsada. Visto este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas: por un lado, resulta excesivamente contaminante para la atmósfera, y por otro puede axfisiar a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón aunque se siguen utilizando mucho hoy en día por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un pitido.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos. Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero hemos de recordar que puede existir humo sin necesidad de que haya un fuego por ejemplo, en salas de operaciones donde se fuma. Aunque muchos no apliquemos esta regla y fumemos demasiado siempre es demasiado delante de nuestros equipos, sería conveniente no permitir esto aparte de la suciedad generada que se deposita en todas las partes de un ordenador, desde el teclado hasta el monitor, generalmente todos tenemos el cenicero cerca de los equipos, por lo que el humo afecta directamente a todos los componentes incluso al ser algo más habitual que un incendio, se puede considerar más perjudicial para los equipos y las personas el humo del tabaco que el de un fuego.

En muchos manuales de seguridad se insta a los usuarios, administradores, o al personal en general a intentar controlar el fuego y salvar el equipamiento; esto tiene, como casi todo sus pros y sus contras. Evidentemente algo lógico cuando

estamos ante un incendio de pequeñas dimensiones es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente. Sin embargo, cuando las dimensiones de las llamas son considerables lo último que debemos hacer es intentar controlar el fuego nosotros mismos, arriesgando vidas para salvar hardware como sucedía en el caso de inundaciones, no importa el precio de nuestros equipos o el valor de nuestra información nunca serán tan importantes como una vida humana. Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar su control en manos de personal especializado.

2.2.6.4.- TEMPERATURAS EXTREMAS

No hace falta ser un genio para comprender que las temperaturas extremas, ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas, para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un acondicionador de aire, aparato que también influirá positivamente en el rendimiento de los usuarios las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente. Otra condición básica para el correcto funcionamiento de cualquier equipo que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU. La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

2.3.- SEGURIDADES EN LAS COMUNICACIONES

Es un hecho conocido que Internet constituye un canal de comunicaciones inseguro, debido a que la información que circula a través de esta vasta red es fácilmente accesible en cualquier punto intermedio por un posible atacante, en

esta parte del capitulo trataremos un tema que es muy árido como es la seguridad en Internet y como debemos protegernos.

2.3.1.- LA NECESIDAD DE UN CANAL SEGURO

Los datos transmitidos entre dos nodos de Internet por ejemplo su máquina y el servidor Web desde el que quiere descargar una página se segmentan en pequeños paquetes que son encaminados a través de un número variable de nodos intermedios hasta que alcanzan su destino. En cualquiera de ellos es posible leer el contenido de los paquetes, destruirlo e incluso modificarlo, posibilitando todo tipo de ataques contra la confidencialidad y la integridad de sus datos. El símil más conocido y gráfico para ilustrar esta situación es el de la tarjeta postal, que puede ser fisgada por los empleados de correos, por los vecinos o por la familia, por lo que no suele confiársele información sensible. Ahora bien, ¿qué se puede hacer en el caso de que se necesite enviar datos confidenciales? Se utilizaría un sobre cerrado y lacrado. En el caso de Internet, la solución más comúnmente adoptada para construir el análogo digital de este sobre se basa en la utilización del protocolo SSL (Secure Sockets Layer), éste es un protocolo desarrollado por Netscape Communications para cifrar información al enviarla por la red.

Más adelante en el Capitulo III E-Commerce veremos más a fondo este protocolo el cual utilizaremos para poder tener mayor confidencialidad al momento de enviar formularios.

2.4.- SEGURIDADES EN EL SERVIDOR

Hoy en día las conexiones a servidores Web son sin duda las más extendidas entre usuarios de Internet, hasta el punto de que muchas personas piensan que este servicio (HTTP, puerto 80 TCP) es el único que existe en la red junto al IRC

Lo que en un principio se diseñó para que unos cuantos físicos intercambiaran y consultaran artículos fácilmente, en la actualidad mueve a diario millones de dólares y es uno de los pilares fundamentales de cualquier empresa es por tanto un objetivo muy atractivo para cualquier pirata.

Los problemas de seguridad relacionados con el protocolo HTTP se dividen en tres grandes grupos en función de los datos a los que pueden afectar:

– Seguridad en el servidor

Es necesario garantizar que la información almacenada en la máquina servidora no pueda ser modificada sin autorización, que permanezca disponible y que sólo pueda ser accedida por los usuarios a los que les esté legítimamente permitido.

– Seguridad en la red

Cuando un usuario conecta a un servidor Web se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente desde el servidor sean los mismos que se están enviando (esto es, que no sufran modificaciones de terceros), y también garantizar que la información que el usuario envía hacia el servidor no sea capturada, destruida o modificada por un atacante. Esto es especialmente importante si la información en tránsito es secreta, como en el caso de los passwords que el usuario teclea para autenticarse en el servidor, o en el comercio electrónico y el intercambio de números de tarjetas de crédito.

– Seguridad en el cliente.

Por último es necesario garantizar al usuario que lo que descarga de un servidor no va a perjudicar a la seguridad de su equipo sin llegar a extremos de applets maliciosos o programas con virus, si simplemente el navegador del usuario se cuelga al acceder al visitar las páginas de una organización, seguramente esa persona dejará de visitarlas, con la consecuente pérdida de imagen y posiblemente de un futuro cliente para esa entidad.

Asegurar el servidor implica aparte de las medidas habituales para cualquier máquina medidas excepcionales dedicadas al demonio servidor de Web y su entorno de trabajo; estas medidas son propias para cada programa servidor, por lo que aquí no entraremos en detalles concretos sobre cada uno de ellos. No obstante, y sea cual sea el servidor utilizado (Apache, NCSA, Netscape, entre otros), es necesario seguir un consejo básico minimizar el número de usuarios en la máquina y minimizar el número de servicios ofrecidos en ella aunque lo normal es que una máquina dedicada a cualquier tarea con decenas o con miles de usuarios sea también el servidor Web, es recomendable que dicho servidor sea un equipo dedicado a esa tarea.

Los problemas relacionados con servidores Web suelen proceder de errores de programación en los CGIs ubicados en el servidor. Un CGI (Common Gateway Interface) es un código capaz de comunicarse con aplicaciones del servidor, de forma que desde una página se invoque a dichas aplicaciones pasándoles argumentos y el resultado se muestre en el navegador de un cliente cuando rellenamos un formulario, vemos una imagen sensible, o simplemente incrementamos el contador de cierta página, estamos utilizando CGIs. Esta capacidad del CGI para comunicarse con el resto del sistema que alberga las páginas es lo que le otorga su potencia, pero también lo que causa mayores problemas de seguridad un fallo en estos programas suele permitir a cualquier visitante de las páginas ejecutar órdenes en el sistema. Los errores más habituales en un CGI provienen de los datos recibidos desde el navegador del cliente un simple formulario, en el que el visitante rellena ciertos campos, puede ser una puerta de acceso a nuestro sistema es necesario comprobar la validez de todos y cada uno de los datos leídos antes de que sean procesados. Por ejemplo, imaginemos un CGI que pida un nombre de usuario por teclado y a continuación ejecute un finger contra ese nombre de usuario y muestre el resultado en el navegador que sucedería si el visitante introduce como nombre de usuario `toni;cat /etc/passwd'? Es posible que se ejecute el finger a toni, pero a continuación se vuelque el fichero de contraseñas simplemente porque no se ha tenido la precaución de ignorar los caracteres especiales para el shell

(recordemos que un en Linux separa varias órdenes en una misma línea); este ejemplo, que hoy en día parece absurdo, ha estado presente en algunos servidores durante mucho tiempo. Cualquier CGI es susceptible de presentar problemas de seguridad sin importar el lenguaje en que se haya escrito por tanto, es muy importante preocuparse de mantener actualizado el árbol de CGIs (no copiarlo completamente al actualizar la versión de demonio), e incluso revisar los programas más importantes en busca de posibles bugs. Otra medida de seguridad básica es ejecutar el demonio servidor bajo la identidad de un usuario con privilegios mínimos para que todo funcione correctamente, pero nunca como root generalmente, el usuario nobody suele ser más que suficiente recordemos que los CGIs se ejecutan bajo la identidad del usuario propietario del demonio, por lo que si ese propietario es el administrador un potencial atacante podría ejecutar cualquier aplicación como root del sistema.

Para garantizar la seguridad de los datos que circulan entre un cliente y el servidor es casi obligatorio cifrar dichos datos (otras medidas, como asegurar físicamente la red, suelen ser impracticables) mediante SSL (Secure Socket Layer), un protocolo desarrollado por Netscape Communications para cifrar información al enviarla por la red y descifrarla antes de ser utilizada en el cliente; en la actualidad, se está viendo relegado a un segundo plano a causa de los certificados digitales, aunque sigue siendo una excelente opción para administración remota y para transmitir información confidencial en redes de propósito general.

En último lugar es necesario hablar de la seguridad desde el punto de vista del cliente que visita páginas Web para el usuario, un servidor es seguro si protege la información que recibe y envía hacia él, manteniendo su privacidad, y si no conduce al usuario a descargar programas maliciosos generalmente virus en su equipo si sucede lo contrario, la compañía responsable de las páginas se enfrenta a una importante pérdida de imagen aparte de posibles problemas judiciales de cara a sus usuarios simplemente imaginemos que salta a los medios un fallo de seguridad en la versión electrónica de cierto banco será difícil que todos sus

usuarios sigan manteniendo la suficiente confianza en él como para guardar allí su dinero. También es necesario hablar de los applets hostiles o simplemente de los mal diseñados que en muchas ocasiones llegan a detener todas las copias del navegador en memoria aunque sus implicaciones de seguridad no suelen ser muy graves, la pérdida de imagen de la compañía es también considerable en estos casos.

En muy pocas máquinas se pueden permitir el lujo de deshabilitar este servicio, ya que como hemos dicho es de los más utilizados actualmente; no obstante, por alguna extraña razón personalmente no la llego a comprender en algunos clones de Unix (por ejemplo, ciertas variantes de Linux) el servicio HTTP está activado por defecto aún a sabiendas de que muchos de los usuarios de este sistema van a utilizarlo en su casa o como estación de trabajo independiente, donde evidentemente no es habitual ni necesario en la mayoría de ocasiones ofrecerlo. Por supuesto, en estos casos es importante detener el demonio httpd y evitar que se vuelva a iniciar con el arranque de la máquina, modificando el script correspondiente. Siempre hemos de recordar que hemos de ofrecer sólo los servicios imprescindibles en cada sistema.

2.5.- CERTIFICADOS DE AUTENTICIDAD

Aunque nuestros datos viajen cifrados por la Red, si los estamos enviando a o recibimos de un impostor, no saldremos mucho mejor parados. Se hace imprescindible el contar con un mecanismo que dé fe de si un servidor seguro es quien creemos que es y podemos confiar en él a la hora de transmitirle nuestra información. La forma como se hace es mediante las CA (Autoridades de Certificación), conocidas informalmente como notarios electrónicos, encargadas de autenticar a los participantes en transacciones y comunicaciones a través de la Red. Su función es emitir certificados a los usuarios, de manera que se pueda estar seguro de que el interlocutor (cliente o servidor) es quien pretende ser, garantizando así la seguridad de las transacciones.

El certificado de seguridad se concede a una entidad después de comprobar una serie de referencias, para asegurar la identidad del receptor de los datos cifrados. Se construye a partir de la clave pública del servidor solicitante, junto con algunos datos básicos del mismo y es firmado por la autoridad de certificación correspondiente con su clave privada. Para hacer a sus clientes sentirse seguros en su Web, su servidor Web necesita ser seguro. Los servidores seguros usan el protocolo SSL, que en cripta los datos al mandarlos entre un browser y el servidor. Cuando su browser se comunica usando SSL, vera el prefijo https: antes URL (Uniform Resource Locator), en la barra de navegación.

Los clientes se sienten mejor cuando hacen las compras desde sitio Web donde saben que sus transacciones son seguras, pero los servidores seguros solo son usados para el comercio electrónico. Un servidor seguro puede ser usado también para transmitir datos sensibles. Un servidor seguro usa un certificado para identificarse a los browser de la Web. Puede generar su propio certificado (llamado un certificado "self-signed") o puede coger un certificado desde un Certificate Authority o CA. Un certificado desde un CA honrado garantiza que un sito Web esta relacionado con una compañía particular o organización.

Si su servidor será usado para e-commerce, probablemente quiera compara un certificado desde una CA. Un certificado CA proporciona dos ventajas: normalmente los browsers lo reconocen automáticamente y el CA garantiza la identidad de la organización responsable para el sito Web. Los certificados Self-signed no son automáticamente aceptador por un browser de usuarios el usuario será preguntado por el browser si quiere aceptar el certificado y crear una conexión segura.

Cuando use un certificado CA-signed, garantiza la identidad de la organización. Por ejemplo, si el certificado dice el sitio Web es Red Hat y el usuario confía en la CA, entonces no hay razón para dudar que la descarga de los fichero o programas son realmente de este sitio.

2.5.1.- ¿QUE ES UNA AUTORIDAD DE CERTIFICACIÓN?

Es esa tercera parte fiable que acredita la relación entre una determinada clave y su propietario real. Actuará como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Sin embargo ¿quién autoriza a dicha autoridad?, es decir, ¿cómo sé que la autoridad es quién dice ser?, ¿Deberá existir una autoridad en la cúspide de la pirámide de autoridades certificadoras que posibilite la autenticación de las demás?.

Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser fiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave. Esta solución da origen a diferentes niveles o jerarquías de CA.

En cuanto a los Certificados, son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.

Contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificarte, el número de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un Registro, considerado como una base de datos a la que el público puede acceder directamente en línea (on-line) para conocer acerca de la validez de los mismos. Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.

La Autoridad Certificante puede emitir distintos tipos de certificados:

- Certificados de identificación: identifican y conectan un nombre a una clave pública

- Certificados de autorización: ofrecen otro tipo de información correspondiente al usuario, como por ejemplo la dirección comercial, antecedentes, catálogos de productos, entre otros.

- Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para dar fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.

- Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (Digital time).

El interesado en operar dentro del esquema establecido por la ley, deberá, una vez creado el par de claves, presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita 'firmar' el documento de que se trate. Por ejemplo, para realizar una operación financiera de importancia con un banco, Este puede requerir al interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado solo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

Los Registros son la base de datos a la que el público puede acceder on-line para conocer la validez de los certificados, su vigencia o cualquier otra circunstancia que se relacione con los mismos. Dicha base de datos debe incluir, entre otras cosas, los certificados publicados en el repositorio, las notificaciones de certificados suspendidos o revocados publicadas por las autoridades

certificantes acreditadas y los archivos de autoridades certificantes autorizadas y todo otro requisito exigido por la Ley. Para ser reconocido, el repositorio debe operar bajo la dirección de una autoridad certificante acreditada.

Es por tanto objeto de esta ley el regularizar la actividad de dichas autoridades o proveedores de servicios de certificación, con la Firma Electrónica se permite asegurar la identidad electrónica tanto de la persona física como de la jurídica. Aporta un marco legal idóneo para las relaciones entre el consumidor, la empresa y la administración. De esta forma se establece el punto de partida para el desarrollo del Comercio Electrónico. Analizando, vemos que tiene por objeto regular el uso de la Firma Electrónica, el reconocimiento de su eficacia jurídica, así como regularizar a las autoridades u organismos en la actividad de servicios de certificación. Para ello, define el concepto de Firma Electrónica, establece sus efectos jurídicos y regulariza la situación legal de los prestadores de dichos servicios de certificación.

2.5.2.- ¿CÓMO RECONOCER QUE EL SITIO ES SEGURO?

En la práctica, sabremos que el servidor es seguro porque en nuestro navegador veremos una llave  o un candado cerrado en la parte izquierda, si usamos Netscape, o bien un candado cerrado en la parte derecha  , si usamos el Explorer.

Advertencia: Una llave entera o un candado cerrado no garantizan una comunicación segura. Es necesario comprobar el certificado, otro cambio importante es el identificador de protocolo en la URL, que varía ligeramente: ya no empieza con http, sino con https.

2.6.- ASEGURANDO LA APLICACIÓN

En el mundo de hoy las aplicaciones Web se han convertido en una forma rápida e independiente de la plataforma para lograr entregar soluciones al usuario

final, estas aplicaciones por sus características pueden o no ser de uso publico, pero finalmente las soluciones y la información que comunican, puede ser privada uno de los principales objetivos en mantenerla así, aquí se tratara de las características básicas para el diseño de una aplicación Web y mantener la información tan privada como sea posible.

Uno de los temas mas espinosos cuando se diseña una aplicación tipo Web, es la seguridad y como garantizarla, desde el principio del diseño debe intentarse identificar cual será la información que se pretende mantener confidencial, y que parte de toda información disponible requiere acceso restringido. Esta es la parte inicial de establecer un perfil de seguridad, para establecer un verdadero perfil de seguridad en una aplicación se deben establecer los siguientes:

- Definir los tipos de información disponibles dentro de su aplicación.
- Definir los métodos de acceso a la misma. Ej.: paginas html, correo electrónico PDF
- Métodos de autenticación para tener acceso a la información. Ej.: Log y password, Log y smardcard, etc.
- Perfiles de los usuarios del sistema, requerimientos de información.
- Crear grupos de usuarios de acuerdo a los perfiles construidos

Una vez ha definido los perfiles y las características básicas que tendrá una usuario en la red, debe decidir que sistema de autenticación usara y como lo ha de implementar en la red. Algunos de los sistemas de autenticación disponibles son:

- Log y password: este sistema tiene la ventaja de ser simple de implementar, permita una autenticación básica dado que el sistema es bastante popular es el que as intentos de ataques sufre por parte de usuarios no autorizados.
- Log y Smartcards, este sistema permite por medio de un dispositivo digital tipo tarjeta generar un password único por sección, permite un alto grado de seguridad ya que el password es único e irrepetible a lo largo del uso del

mismo. Dados los costos no es muy popular en el momento pero brinda un alto grado de confiabilidad.

- Sistemas biométricos: dado el costo es el menos popular pero permite crear un sistema de acceso extremadamente segura que en un entorno de alto riesgo puede ser la opción ideal, entre estos sistemas se encuentran huellas digitales identificación vocal o retinal.
- Certificados digitales: dados los bajos costos en la compra de un certificado digital en entorno muy dispersos se presenta como la alternativa ideal para autenticación remota, debe tenerse cuidado con la copia de los certificados, pero en general es un sistema de bastante aceptación y gran eficacia.

Teniendo autenticado el usuario debemos evitar que la información pueda ser alterada o vista por personas que no deben tener permiso a ello, la forma más común para garantizar esto es la criptografía, pero a nivel de Web existen dos formas que permiten hacerlo sin problemas o altos costos, algunos de este sistema son:

- SSL: es el sistema más popular que existe en este momento, dado su simplicidad de implementación y mantenimiento requiere por parte del servidor o proveedor de la información la compara de un certificado digital en caso publico. En el caso de redes privadas la implantación de una entidad certificadora (CA), que toda la red pueda confiar. Es de particular importancia que se implemente de manera adecuada dado que una mala implementación puede conducir a que el sistema no funcione correctamente y/o de manera segura.

- VPN (virtual private network) es el sistema de autenticación preferido en el caso de entidades financieras, empresas que tengan redes de área extendida (WAN) dado su alta seguridad y que los sistemas en este tipo de red pueden usar redes públicas de bajo costo para implantar su sistema de comunicaciones. Casi siempre van acompañados de sistema de firewall.

Son sistemas en un rango de precio mas alto y pueden llegar a hacer por esto prohibido en determinados entornos.

– Finalmente pero no menos importante recuerde colocar la mínima cantidad de formas de entrada a su sistema, en lo posible un único punto es lo mas aconsejable dado que de esa forma podrá minimizar los riesgos naturales de implementación y facilitara el control por parte de los administradores de la red.

2.7.- CASO DE ESTUDIO INTEGRAR S.A ASP ESPAÑOL [1]

ASP/Integrar ofrece un Outsourcing completo de sistematización, a través de una red privada de comunicaciones, para las empresas medianas y pequeñas cuyas necesidades y requerimientos tecnológicos son los mismos de las grandes corporaciones, pero que no cuentan con cifras de facturación suficientes para absorber dichos costos.

Con el servicio prestado por ASP/Integrar, usted puede concentrar su tiempo y sus recursos en la razón de ser de su negocio y por una suma mensual, recibir el nivel de servicio que requiere para operar eficientemente.

CÓMO FUNCIONA ASP/INTEGRAR

Las empresas sólo requieren del personal necesario para operar el aplicativo desde sus propias instalaciones. A través de una red privada de comunicaciones con tecnología VPN, la información se almacena y procesa en un sofisticado

[1] www.integrar.com.co/ASP/ASP.htm

Centro de Datos construido y administrado con los más altos estándares de seguridad y tecnología.

Figura II-2 Diagrama de Conexión de ASP INTEGRAR S.A

Está construido en un edificio aislado de edificios vecinos, con una estructura sismorresistente, con las mas exigentes medidas de seguridad para el acceso, como puerta blindada accionable solamente a través de tarjeta y clave a personal autorizado, cámaras de televisión monitoreadas y filmadas permanentemente y un división de vidrio blindado para aislar el área donde se alojan los servidores. Cuenta con piso falso, aire acondicionado de precisión para asegurar la temperatura y la humedad constantes, techo falso, acometida eléctrica independiente, equipos de potencia ininterrumpida (UPS) de última tecnología para garantizar la operación 24 horas del día los 365 días del año, se cuenta además con Servidores en Cluster (soporte entre ellos en caso de caída), planta eléctrica capaz de soportar la operación por varios días en caso de falla del fluido eléctrico normal, copias de seguridad (back-up) automático y en caliente, y un equipo detector y extintor de incendios con elemento activo FM200. Operadores e ingenieros calificados y expertos en los diferentes temas como bases de datos, sistemas operativos, software aplicativo y línea telefónica privada, están permanentemente monitoreando la operación.

Figura II-3 Centro de Datos de INTEGRAR S.A

Capitulo

3

III.- E-COMMERCE

La presente introducción al comercio electrónico se ha diseñado con el fin de dar una visión general de los conceptos más comunes, algunos de los cuales se desarrollan de forma más detallada en el capitulo, mas adelante veremos las formas de pago más extendidos hoy en día, para comprar en línea de forma completamente fiable y segura.

En la actualidad, resulta evidente que hasta las pequeñas y medianas empresas deben enfrentarse al reto de la adopción del comercio electrónico. Presenta grandes ventajas a aquellos que sean lo suficientemente valientes como para asumir el desafío, desde la protección de una posición existente en el mercado hasta el desarrollo de un nuevo negocio electrónico.

3.1.- E-COMMERCE

¿Qué es el comercio electrónico?

El Comercio Electrónico o e-commerce es el intercambio y procesamiento de información sobre transacciones comerciales a través de computadores conectados a una red. Entre otros ejemplos de tales transacciones están la selección de artículos, la realización de pedidos, la facturación y los pagos. Con frecuencia, la red que se utiliza como enlace es Internet, pero también puede ser una red privada. Se puede hacer una diferenciación entre el comercio electrónico, que a menudo representa la solución electrónica de cara a los clientes y el e-business, término que suele abarcar la integración de tales soluciones de cara a los clientes con sistemas de respaldo en las oficinas.

Aunque comercio electrónico es la expresión de moda, se lleva años realizando transacciones electrónicas. Hace más de dos décadas, hubo grandes empresas que empezaron a utilizar un sistema llamado EDI (Intercambio de Datos Electrónicos). También las instituciones financieras llevan tiempo moviendo sus activos de forma electrónica. Estas primeras generaciones de sistemas electrónicos tuvieron un gran inconveniente eran caras de usar y de poner en marcha. El éxito del comercio electrónico, tal como lo conocemos hoy en día, se debe en gran medida al éxito de Internet: una red barata y de escala planetaria que conecta a millones de personas y negocios, creando de este modo un verdadero *mercado global.*

3.1.1.- B2C (BUSINESS TO CONSUMER)

El ASP B2C brinda un servicio de comercio electrónico entre empresas y un usuario final de fácil aplicación.

3.1.1.1.- Beneficios del ASP B2C

B2C permite que usted construya un canal de venta digital en donde los compradores pueden operar diariamente para comprar grandes cantidades mercancías. El usuario se sentirá a gusto comprando cómodamente desde su hogar, buscando productos deseados, leyendo información acerca de los mismos y agregándolos al carrito de compras como si fuera una experiencia real.
Los beneficios concretos son:

- Bajar los costos de transacción
- Reducción de los inventarios
- Optimización los recursos
- Transacciones las 24 horas del día
- Acceso desde cualquier parte con un Web browser
- Seguimiento de los pedidos vía Web
- Estadísticas e historiales de ventas

- Catálogos de productos
- Conveniencia y eficiencia para el comprador
- Reducción de costos internos
- Reducción de tiempos

3.1.2.- B2B (BUSINESS TO BUSINESS)

Este concepto representa el mayor potencial para impactar a los negocios alrededor de su estrategia de Internet. El e-business necesariamente involucra y redefine los procesos de negocio de cualquier empresa y su cadena de valor. No es que se quiera subestimar a Internet B2C (de negocio a último consumidor) sino que en buena medida las empresas han subestimado al B2B. A continuación algunos datos.Según el Forrester Group, las transacciones de B2B en Estados Unidos se incrementarán de 43 billones de dólares en el 98 al trillón en el 2003, mientras que las de business to consumer pasarán de 7.8 billones de dólares a 108 billones.

Podemos identificar por lo menos cuatro grupos de componentes, según un reportaje aparecido en el New York Times/Bob Tedeschi, el 7 de Mayo del 2000.

- Infraestructura y Arquitectura: Tras la debacle del Nasdaq, Independientemente de quien sobreviva finalmente, si B2C, B2B, o B2A (business to anyone), hay un claro ganador: la infraestructura que demandarán tanto el e-business como el e-commerce. Hardware, ruteadores, software y tecnologías que mueven inmensas cantidades de datos de información Cisco, Sun, Oracle, Microsoft y el EMC Corporation son algunos ejemplos. Con la aceleración de Internet, muchas compañías se han percatado de la necesidad de hacer outsourcing de infraestructura de sistemas o de contratar lo servicios de un ASP, los expertos estiman que las empresas estadounidenses se verán obligadas a hacerlo hasta en

un 50 por ciento de los casos, claramente marcando el inicio de una tendencia mundial

- Software relacionado a transacciones B2B: Una vez montada la infraestructura, se necesita el software y las aplicaciones para que se dé la transmisión de información, bases de datos, captura de transacciones, manejo de relaciones con clientes (CRM), comercio electrónico, promociones en línea, etcétera.Alrededor del software de B2B están varios jugadores, desde desarrolladores, comercializadores, e integradores de sistemas

- Consultoría: Muchas empresas deciden buscar intermediarios o consultores que colaboren en el peregrinaje de la vieja economía a la nueva economía, y es que estar en Internet es mucho más que montar una página Web esto es apenas el primer paso. El segundo paso lógico después de tener un domicilio en la web, es el desarrollo de Intranet donde ciertos procesos internos se manejen y se hagan más eficientes, como por ejemplo el flujo de información de/hacia/para la fuerza de ventas la Extranet, es el tercer paso típico y normalmente involucra comunicación hacia fuera de la organización, con clientes y/o proveedores, finalmente viene la fase de comercio, que se facilita bastante cuando la empresa ya maneja varios procesos desde las primeras fases, conviene aclarar en Internet no hay reglas claras y abundan los casos donde con sus riesgos y beneficios se da el brinco de la fase uno a la cuatro, de golpe

- Intercambios o Marketplaces: Estos han sido los verdaderos disparadores del B2B. Los marketplaces se pueden dividir en dos tipos: el de bienes directos o insumos y el de indirectos. En primer caso, los productos que se manejan son el correo la esencia del negocio. Algunos ejemplos: Chedmex.com, E-steel.com. Construmega.com. A su vez, los tres grandes de los autos: Ford, General Motors y Chrysler están formando el mercado

de intercambios de autopartes, donde están obligando a los proveedores a hacerlo en línea.

En el segundo caso de este rubro está el marketplace de los productos indirectos. Aquí se pueden comprar bienes, por ejemplo, de mantenimiento, reparación, viajes y artículos de oficina. Todas las compañías pueden participar de este mercado y obtener las eficiencias de comprar bajo este esquema, en México ya hay por lo menos dos compañías que iniciaron con este concepto Commerce One-Banamex y Asista.com.

Las ventajas de adoptar algún esquema de B2B como medio de mejora se puede resumir en un comunicado de prensa con las declaraciones de Jesús Herrera, Director de Key Química "creemos que ganaremos una ventaja competitiva al reducir el tiempo de nuestro ciclo de compra aproximadamente en un 70% por ciento, al moverse a la solución B2B de comercio electrónico de Asista.com" y agrego "estamos emocionados de ser los pioneros en esta tendencia mundial, y que nos permitirá hacer más eficientes nuestros procesos de comercio al lograr economías de escala y ahorros".

3.1.2.1.- Beneficios del ASP B2B

B2B permite que usted construya canales de venta digitales en donde los compradores y los distribuidores pueden operar diariamente para mover grandes cantidades mercancías. La tecnología que utiliza el B2B para realizar las transacciones se puede aplicar para: planear colaborativamente a través de su cadena de proveedores; compartir diseños en el desarrollo de un nuevo producto, así como la logística para coordinar, obtener, producir y entregar los materiales y los productos.

- Los beneficios concretos son:
- Bajar los costos de transacción

- Reducción de los inventarios
- Optimización los recursos
- Reducción el tiempo de salida de los productos al mercado
- Transacciones las 24 horas del día
- Acceso desde cualquier parte con un Web browser
- Seguimiento de los pedidos vía Web
- Estadísticas e historiales de ventas
- Catálogos privados de productos
- Conveniencia y eficiencia para el comprador
- Reducción de costos internos
- Reducción de costos de distribución
- Reducción de tiempos

3.2.- MEDIOS DE PAGO EN INTERNET

El comercio electrónico en Internet constituye una compleja ecuación cuyas principales incógnitas a despejar son: una mercancía que vender, conseguir que compradores potenciales conozcan su existencia, aceptar su pago en caso de venta, entregar los bienes o servicios adquiridos y ofrecer un servicio posventa.
La mayoría de las empresas comenzaron por crear sitios Web de presencia en Internet, como medio eficaz para dar a conocer su oferta de productos y servicios y atraer nuevos clientes, incluso a escala mundial. En esa etapa, la mayor parte de las compras reales tenían lugar fuera de la Red, que servía a lo sumo como escaparate virtual para poner en relación al comprador y vendedor. Con la aparición progresiva de nuevos medios de pago digitales, se está posibilitando la existencia de transacciones comerciales realizadas completamente a través de Internet. Una vez efectuado el pago, el comerciante envía los artículos adquiridos contratando los servicios de una empresa de paquetería, en el caso de bienes físicos (hardware), o bien directamente vía Web en el caso de bienes digitales, como información o programas (software), abaratando drásticamente en este caso los costes de distribución. El servicio posventa puede ofrecerse igualmente en línea.

En esta cadena comercial de valor, el eslabón más débil ha sido, y todavía es, la forma de pago, el mayor obstáculo tanto técnico como psicológico que debe ser vencido para que se produzca el despegue definitivo del comercio electrónico. Mientras no exista confianza, mientras los usuarios teman al fraude, mientras se desconozcan los sistemas de pago empleados y su fiabilidad, es difícil que se observe un incremento sustancial en esta novedosa forma de comercio.

En los últimos cinco años ha ido surgiendo un número considerable de tecnologías y sistemas de pago electrónico que ofrecen las garantías de seguridad e integridad necesarias para realizar las compras en línea de una manera fiable y sin sorpresas. La piedra angular de todas ellas es la criptografía, que proporciona los mecanismos necesarios para asegurar la confidencialidad e integridad de las transacciones. Se verá a continuación en qué consisten estos protocolos y cómo proporcionan la seguridad requerida.

3.2.1.- SSL (SECURE SOCKETS LAYER)

Este protocolo fue diseñado y propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator. Sin embargo, no fue hasta su tercera versión, conocida como SSL v3.0 que alcanzó su madurez, superando los problemas de seguridad y limitaciones de sus predecesores. En su estado actual, proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

SSL v3.0 goza de gran popularidad, por lo que se encuentra ampliamente extendido en Internet. Viene soportado por los dos principales navegadores del mercado, Netscape Navigator 3.0 ó superior, así como por Internet Explorer 3.0 ó superior, no se necesita realizar ninguna acción especial para invocar el protocolo SSL, basta con seguir un enlace o abrir una página cuya dirección empieza por https://. El navegador se encarga del resto. Eso sí, asegúrese de que tiene SSL habilitado en su navegador.

3.2.1.1.- CÓMO FUNCIONA SSL

El rasgo que distingue a SSL de otros protocolos para comunicaciones seguras, como el hoy prácticamente extinto S-HTTP, es que se ubica en la pila OSI entre los niveles de transporte (TCP/IP) y de aplicación (donde se encuentran los conocidos protocolos HTTP para Web, FTP para transferencia de ficheros, SMTP para correo electrónico, Telnet para conexión a máquinas remotas, etc.). Gracias a esta característica, SSL resulta muy flexible, ya que puede servir para securizar potencialmente otros servicios además de HTTP para Web, sin más que hacer pequeñas modificaciones en el programa que utilice el protocolo de transporte de datos TCP.

SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 o IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 o SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes fases (de manera muy resumida):

1. La fase Hola, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles.

Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.

2. La fase de autenticación, en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).
3. La fase de creación de clave de sesión, en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.
4. Por último, la fase Fin, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores) a través del cual se intercambiará cifrada la información relevante, como el URL y los contenidos del documento solicitado, los contenidos de cualquier formulario enviado desde el navegador, las cookies enviadas desde el navegador al servidor y viceversa y los contenidos de las cabeceras http.

3.2.1.2.- USO DE SSL EN COMERCIO ELECTRÓNICO

SSL constituye la solución de seguridad implantada en la mayoría de los servidores Web que ofrecen servicios de comercio electrónico. Su mayor mérito

radica en ofrecer respuesta al principal problema que afronta el comercio en línea: la renuencia de los usuarios a enviar su número de tarjeta de crédito a través de un formulario Web por el temor de que caiga en manos de un hacker y por la desconfianza generalizada hacia Internet.

La forma más fácil y más extendida para construir un sistema de comercio en Internet consiste en utilizar un servidor Web con un catálogo con información sobre los productos o servicios ofrecidos y un formulario para procesar los pedidos. El catálogo estará compuesto por una serie de páginas Web describiendo la mercancía en venta, acompañadas de imágenes, dibujos, especificaciones, animaciones, clips de vídeo o audio, applets de Java, controles ActiveX, etc. Estas páginas Web se pueden crear estáticamente con un programa de edición HTML como Microsoft FrontPage o Adobe PageMill, o también pueden crearse dinámicamente desde una base de datos de los artículos y su información asociada, con programas como FileMaker Pro de Claris. Junto a cada artículo se sitúa un botón que el usuario puede pulsar para comprarlo o, más comúnmente, para añadirlo al carrito de la compra para pagarlo todo al final. Cuando el cliente ha terminado sus compras, pasa por una "caja virtual", que iniciará el proceso de pago.

Hoy por hoy, el medio de pago más común en Internet es la tarjeta de crédito, no hay que despreciar otros métodos más conservadores, aunque a menudo preferidos por los compradores, como el envío contra reembolso o la transferencia bancaria, que representan un porcentaje importante de las ventas en línea. El usuario debe rellenar un formulario con sus datos personales (tanto para el caso del envío de los bienes comprados, como para comprobar la veracidad de la información de pago), y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. *Basta con que se utilice como mínimo un canal seguro para transmitir la información de pago y el comerciante ya se ocupará manualmente de gestionar con su banco las compras.*

Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura. A medida que el comercio crece, esta arquitectura podría llegar a resultar difícil de expandir o de incorporar nuevas tecnologías y componentes a medida que vayan apareciendo. Existen una serie de desventajas al utilizar exclusivamente SSL para llevar adelante ventas por Internet.

– Por un lado, SSL ofrece un canal seguro para el envío de números de tarjeta de crédito, pero carece de capacidad para completar el resto del proceso comercial: verificar la validez del número de tarjeta recibido, autorizar la transacción con el banco del cliente, y procesar el resto de la operación con el banco adquiriente y emisor.

– Por otro lado, es importante recalcar que SSL sólo garantiza la confidencialidad e integridad de los datos en tránsito, ni antes ni después. Por lo tanto, si se envían datos personales al servidor, entre ellos el ya citado número de tarjeta de crédito, el número de la seguridad social, el DNI, etc., SSL solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltara el servidor con éxito.

– Además, SSL permite realizar ataques sobre servidores de comercio creados sin las medidas de seguridad, para averiguar números de tarjeta reales. Un programa escrito por el hacker va probando números de tarjeta válidos, pero que no se sabe si corresponden o no a cuentas reales, realizando compras ficticias en numerosos servidores. Si el número de tarjeta no sirve, el servidor devuelve un error, mientras que si es auténtico, el servidor lo acepta. El programa entonces cancela la compra y registra el número averiguado, para seguir adelante con el proceso. De esta forma, el hacker puede hacerse en breve con cientos de números auténticos.

– Todos estos inconvenientes convierten a SSL en una solución deficiente desde el punto de vista del pago electrónico, lo cual no significa que no se deba utilizar ni que no sea útil en otras muchas facetas igualmente necesarias de la actividad empresarial. Al proporcionar un canal seguro de comunicaciones, el comerciante puede ofrecer al cliente de manera confidencial una serie de servicios para estrechar las relaciones de confianza: autenticación del cliente frente al comercio, trato personalizado, evitar que terceras partes espíen las compras de los clientes, intercambio de información privada.

Dado que SSL es un protocolo seguro de propósito general, que no fue diseñado para el comercio en particular, se hace necesaria la existencia de un protocolo específico para el pago. Este protocolo existe y se conoce como SET.

3.2.2.- SET (TRANSACCIONES ELECTRÓNICAS SEGURAS)

Transacciones Electrónicas Seguras (Secure Electronic Transaction o SET) es un protocolo estandarizado y respaldado por la industria, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas, incluyendo Internet. El estándar SET fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, VeriSign y otras.

El 19 de diciembre de 1997 Visa y MasterCard formaron SET Secure Electronic Transaction LLC (comúnmente conocida como "SETCo") para que implantase la especificación. En cuanto el protocolo SET 1.0 fue finalizado, comenzó a emerger una infraestructura basada en el mismo para dar soportar su uso a gran escala. Ya existen numerosos fabricantes de software que han empezado a crear productos para consumidores y comerciantes que deseen realizar sus compras de manera segura disfrutando de las ventajas ofrecidas por SET.

Figura III-1 Logotipo SET

3.2.2.1.- QUÉ SERVICIOS OFRECE SET

– Autenticación: todas las partes implicadas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden autenticarse mutuamente mediante certificados digitales. De esta forma, el comerciante puede asegurarse de la identidad del titular de la tarjeta y el cliente, de la identidad del comerciante. Se evitan así fraudes debidos a usos ilícitos de tarjetas y a falsificaciones de comercios en Internet imitando grandes Web comerciales. Por su parte, los bancos pueden verificar así las identidades del titular y del comerciante.

– Confidencialidad: la información de pago se cifra para que no pueda ser espiada. Es decir, solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere cifrar el resto de datos de la compra, como por ejemplo qué artículos se han comprado, debe recurrirse a un protocolo de nivel inferior como SSL.

– Integridad: garantiza que la información intercambiada, como número de tarjeta, no podrá ser alterada de manera accidental o maliciosa mientras viaja a través de la red. Para lograrlo se utilizan algoritmos de firma digital.

– Gestión del pago: SET gestiona tareas asociadas a la actividad comercial de gran importancia como registró del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, entre otros.

3.2.2.2.- QUIÉNES PARTICIPAN EN SET

El pago mediante tarjeta es un proceso complejo en el cual se ven implicadas varias entidades:

- El banco emisor: emite la tarjeta del cliente, extiende su crédito y es responsable de la facturación, recolección y servicio al consumidor.

- El banco adquiriente: establece una relación con el comerciante, procesando las transacciones con tarjeta y las autorizaciones de pago.

- El titular de la tarjeta: posee la tarjeta emitida por el banco emisor y realiza y paga las compras.

- El comerciante: vende productos, servicios o información y acepta el pago electrónico, que es gestionado por su entidad financiera (adquiriente).

- La pasarela de pagos: mecanismo mediante el cual se procesan y autorizan las transacciones del comerciante. La pasarela puede pertenecer a una entidad financiera (adquiriente) o a un operador de medio de pago, el cual procesa todas las transacciones de un conjunto de entidades.

- El procesador (redes de medios de pago): proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre las que se realizan las transacciones.

- Autoridad de certificación: certifica las claves públicas del titular de la tarjeta, del comerciante y de los bancos.

En una compra convencional mediante tarjeta de crédito, en la que el cliente paga en la tienda haciendo uso de su tarjeta, la transacción sigue los siguientes pasos:

1. El titular de la tarjeta la presenta al comerciante
2. Éste la introduce en el Terminal de Punto de Venta (POST), que su banco le ha proporcionado
3. Los datos de la transacción se envían a través del sistema de redes de medios de pago hasta el banco emisor
4. El banco emisor comprueba que todos los datos son correctos y remite su aprobación
5. De ahí llega al banco adquiriente y al terminal del comercio, de donde saldrá el recibo de la operación
6. El comerciante tendrá ingresado el dinero en su cuenta a las ocho del mañana del día siguiente
7. Por su parte, el cliente no lo verá descontado de su cuenta corriente hasta el mes siguiente, en función de cuándo realice la compra

A continuación se describe cómo SET realiza este mismo proceso a través de Internet.

3.2.2.3.- EL FUNCIONAMIENTO DE SET EN 10 PASOS

Una transacción SET típica funciona de forma muy parecida a una transacción convencional con tarjeta de crédito y consta de los siguientes pasos:

1. Decisión de compra del cliente. El cliente está navegando por el sitio web del comerciante y decide comprar un artículo. Para ello rellenará algún formulario al efecto y posiblemente hará uso de alguna aplicación tipo carrito de la compra, para ir almacenando diversos artículos y pagarlos todos al final. El protocolo SET se inicia cuando el comprador pulsa el botón de Pagar.

2. Arranque del monedero. El servidor del comerciante envía una descripción del pedido que despierta a la aplicación monedero del cliente.

3. El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante. La aplicación monedero crea dos mensajes que envía al comerciante. El primero, la información del pedido, contiene los datos del pedido, mientras que el segundo contiene las instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, etc.) para el banco adquiriente. En este momento, el software monedero del cliente genera un firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente.

4. El comerciante envía la petición de pago a su banco. El software SET en el servidor del comerciante crea una petición de autorización que envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción y otra información relevante acerca de la misma, todo ello convenientemente cifrado y firmado. Entonces se envían al banco adquiriente la petición de autorización junto con las instrucciones de pago (que el comerciante no puede examinar, ya que van cifradas con la clave pública del adquiriente).

5. El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del banco emisor del cliente. El banco del comerciante descifra y verifica la petición de autorización. Si el proceso tiene éxito, obtiene a continuación las instrucciones de pago del cliente, que verifica a su vez, para asegurarse de la identidad del titular de la tarjeta y de la integridad de los datos. Se comprueban los identificadores de la transacción en curso (el

enviado por el comerciante y el codificado en las instrucciones de pago) y, si todo es correcto, se formatea y envía una petición de autorización al banco emisor del cliente a través de la red de medios de pago convencional.

6. El emisor autoriza el pago. El banco emisor verifica todos los datos de la petición y si todo está en orden y el titular de la tarjeta posee crédito, autoriza la transacción.

7. El adquiriente envía al comerciante un testigo de transferencia de fondos. En cuanto el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.

8. El comerciante envía un recibo al monedero del cliente. Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden. El software del servidor almacena la autorización y el testigo de transferencia de fondos. A continuación completa el procesamiento del pedido del titular de la tarjeta, enviando la mercancía o suministrando los servicios pagados.

9. Más adelante, el comerciante usa el testigo de transferencia de fondos para cobrar el importe de la transacción. Después de haber completado el procesamiento del pedido del titular de la tarjeta, el software del comerciante genera una petición de transferencia a su banco, confirmando la realización con éxito de la venta. Como consecuencia, se produce el abono en la cuenta del comerciante.

10. A su debido tiempo, el dinero se descuenta de la cuenta del cliente (cargo).

El protocolo definido por SET especifica el formato de los mensajes, las codificaciones y las operaciones criptográficas que deben usarse. No requiere un método particular de transporte, de manera que los mensajes SET pueden transportarse sobre HTTP en aplicaciones Web, sobre correo electrónico o cualquier otro método. Como los mensajes no necesitan transmitirse en tiempo presente, son posibles implantaciones de SET eficientes basadas en correo electrónico u otros sistemas asíncronos.

En su estado actual SET solamente soporta transacciones con tarjeta de crédito/débito, y no con tarjetas monedero. Se está trabajando en esta línea para extender el estándar de manera que acepte nuevas formas de pago. Al mismo tiempo se están desarrollando proyectos para incluir los certificados SET en las tarjetas inteligentes, de tal forma que el futuro cambio de tarjetas de crédito a tarjetas inteligentes pueda incorporar el estándar SET.

3.2.3.- CYBERCASH

CyberCash, desarrollado en 1994 por CyberCash Corporation, constituye un mecanismo de pago muy similar a SET, que ofrece a los comerciantes una solución rápida y segura para procesar los pagos con tarjeta de crédito a través de Internet.

Al igual que en SET, el usuario necesita utilizar un software de cartera que reside permanentemente en su máquina, como en el caso de Microsoft Wallet o de carteras propietarias de casas de medios de pago o bancos, o bien residen en el servidor de CyberCash, como la cartera de InstaBuy. Por su parte, el comerciante necesita instalar un software en su servidor, Merchant Connection Kit (MCK), parte del sistema global llamado CashRegister 3 Service, que puede adquirirse registrándose en CyberCash e incluye guiones, plantillas y bibliotecas para que los servidores de los comerciantes se conecten al servidor de CyberCash. De esta forma, el comerciante no necesita adquirir un sistema de back-office para el procesamiento de las operaciones de venta con tarjeta, puesto

que es el servidor de CyberCash, y no el del comerciante, el que gestiona con el banco todas las complejas operaciones de pago.

Desde el punto de vista del cliente, esta estrategia le concede mayor seguridad, al implicar que su número de tarjeta nunca llega a ser conocido por el comerciante, sino solamente por el servidor de CyberCash y, por supuesto, por los bancos participantes.

Desde el punto de vista del comerciante, también la seguridad aumenta, ya que el cobro de la mercancía se produce incluso antes de que sea vendida, como ocurre en las transacciones en puntos de venta en las tiendas (de la calle).
Por tanto, puede decirse que CyberCash actúa como intermediario entre el comerciante y el consumidor, asegurando que el primero recibe el pago, mientras que el segundo recibe la mercancía. Por supuesto, por su papel desempeñado en el escenario de compra-venta, carga una pequeña comisión al comerciante, variable en función del volumen de ventas. Con el fin de promover al máximo el uso de CyberCash, tanto el software del cliente como del servidor son gratuitos y están disponibles para múltiples plataformas.

3.2.3.1.- CÓMO PAGAR CON CYBERCASH EN 6 PASOS?

El proceso de pago con CyberCash, que implica al consumidor, al comerciante, el banco emisor y el banco del comerciante, es como sigue:

1. El usuario recorre la tienda virtual hasta que decide comprar un artículo. Entonces se le presenta una página detallando el precio de venta del artículo, gastos de envío y otras condiciones.

2. El consumidor acepta las condiciones al pulsar el botón de pago con CyberCash. En este momento se lanza la aplicación de cartera, en la cual el usuario puede seleccionar la tarjeta con la que pagar. Toda la información del usuario se envía al servidor del comerciante cifrada y

firmada, de manera que no resulte accesible ni manipulable por el comerciante.

3. El comerciante se queda con los datos de envío y de los productos comprados, y envía firmada al servidor de CyberCash la información de pago del cliente, que al estar cifrada por la cartera no ha podido leer.

4. El servidor de CyberCash recibe la petición de transacción y, detrás de su cortafuegos y desconectado de Internet, obtiene del paquete de datos la información de pago del consumidor. Verifica la integridad del pedido recibido del comerciante, verifica la identidad del consumidor y del comerciante, extrae el número de tarjeta del cliente y si todo está en orden, reexpide la transacción al banco del comerciante a través de líneas dedicadas.

5. El banco del comerciante envía una petición de autorización al banco emisor a través de los canales de comunicación tradicionales de las redes de medios de pago, y retransmite a CyberCash la respuesta, afirmativa o negativa del banco del cliente, que autoriza o no el cargo en función del monto de la compra, el crédito disponible y dispuesto, y alguna otra información, como por ejemplo si existen informes de que la tarjeta haya sido robada.

6. CyberCash pasa al comerciante la respuesta del banco, de manera que si es afirmativa, el banco del comerciante recibe el pago del emisor, mientras que si es negativa, se anula la compra, sin riesgo para el comerciante.

Según CyberCash, el proceso completo tarda entre 15 y 20 segundos y en transacciones usando la cartera, nadie excepto el usuario, CyberCash y los bancos ven el número de tarjeta de crédito. Posteriormente, el usuario puede consultar en su cartera el registro de compras, para contrastarlas con la carta del banco informándole de sus cargos en la tarjeta.

La mayor diferencia con SET reside en la madurez y larga andadura de la tecnología de CyberCash, en operación durante más de cinco años, en contraste con SET, que todavía carece de software operativo e interoperable ampliamente disponible, tanto para consumidores como para comerciantes, y se encuentra en fase de pruebas en la mayoría de países. No obstante, CyberCash permite también que los comerciantes, bancos, procesadores de medios de pago y clientes utilicen SET como protocolo de pago.

Capitulo

4

IV.- CONFIGURACIÓN DE UN PROTOTIPO OPERATIVO QUE PERMITA PONER EN MARCHA UN ASP A BAJO COSTO

En este capítulo se establecerá los requerimientos mínimos necesarios para poner en funcionamiento un ASP, además de las direcciones Web donde podemos conseguir el software necesario, para la segunda parte configuraremos los scripts de Linux Red Hat para subir los servicios tales como: Web Server, Application Server, DataBase Server, PPP, Firewall, entre otros, no olvidemos que para un ASP lo más importante es la seguridad de los datos y la disponibilidad de la aplicación.

4.1.- BÚSQUEDA DE ELEMENTOS PARA LA PUESTA EN MARCHA DE UN ASP A BAJO COSTO

A continuación se presentan una breve descripción de las componentes de Hardware y Software que se necesitan para poner en marcha un ASP.

4.1.1.- HARDWARE

El escoger el hardware adecuado es muy importante, puesto que de este dependerá el buen desempeño de la Aplicación, también se debe tener en cuenta el número de clientes que accederán al ASP, y evaluar varios aspectos como los que se listan a continuación:

– Número de clientes: Este es el criterio más importante que debemos tener en cuenta, porque no es lo mismo tener a 10 clientes que tener 100 clientes accesando concurrentemente a nuestra aplicación.

– El número de páginas estáticas (.html, .gif, .jpg) versus las páginas que se generan dinámicamente: Se debe de tener en cuenta que si las páginas están previamente creadas no hay problema, se puede estimar el espacio en disco que van a requerir, el problema se suscita cuando estos 100 clientes están accesando concurrentemente a páginas que son creadas dinámicamente por el Web Server y con datos que son obtenidos de la Base de Datos.

– Tamaño y Diseño de la Base de Datos: De la misma manera que el tiempo de procesamiento se incrementa si existe complejidad en el código se incrementará si existe complejidad en el diseño de la base de datos, de allí el establecer un buen análisis y diseño de las aplicaciones sobre todo de aquellas que van a correr en ambiente WEB.

– Uso de motores de búsqueda: Si se va ha usar un motor de búsqueda se debe de tener en cuenta que el motor de búsqueda creará una base de datos de todas las páginas que tengan metadatos, es decir si un sitio Web tiene aproximadamente 1 GB de páginas se debe de tener por lo menos ell doble de espacio para que se cree la base de datos del motor de búsqueda.

– Uso de encriptación (tecnología SSL): Si se desea dar servicio de e-commerce de seguro que necesitará tener configurado un canal seguro de transmisión de información, esto proporciona SSL, al tener configurado SSL en nuestro servidor cada petición será codificada, este proceso extra de codificación utiliza más recursos.

4.1.1.1- CONFIGURACIÓN DE UN WEB SERVER PEQUEÑO

– Servidor Pentium III de 1 o 2 CPU: Se escoge este tipo de Procesador puesto que es uno de los más estables en el mercado, además por tener gran aceptación y recomendación de los expertos.

– Memoria RAM de 512 MB a 1GB: La cantidad de memoria que se va ha utilizar se la establece luego de hacer un análisis con las herramientas de desarrollo utilizadas, por ejemplo:

1. Un proceso de Apache sin PHP aproximadamente consume 1 MB de memoria.

2. Un proceso de Apache con PHP aproximadamente consume 1.5 MB de Memoria.

3. Un Proceso MYSQL en el cual se realiza una consulta simple a 500,000 registros consume aproximadamente 0.5 a 0.75 MB.

4. Un proceso de Apache con PHP y MYSQL en el cual se realiza un consulta simple a 500,000 registro consume alrededor de 2.25 MB y si 100 clientes están accesando concurrentemente al servidor este consumirán aproximadamente 225 MB de memoria RAM, con esto se justifica la cantidad de memoria recomendada.

– Capacidad en Disco Duro de 20GB a 40GB: La capacidad de almacenamiento va a depender del número de aplicaciones hosteadas y de el número de páginas dinámicas que van a ser generadas, hoy en día no es muy imperioso el cuidar unos bits mas o bits menos, puesto que tenemos discos duros de alta capacidad y a bajos precios.

Ejemplo:

El Servidor ProLiant 360 o 380 es la propuesta de Compaq que reúne las características para poder atender las peticiones de 100 clientes concurrentes, además de la propuesta de Compaq tenemos a IBM con sus equipos de la Serie I.

4.1.2.- SOFTWARE

Todo el Software que se utilizará para la configuración de nuestro ASP es Open Source, se lo puede obtener en el Internet o algunos de los paquetes vienen incluidos en los discos de Instalación de Linux Red Hat.

4.1.2.1.- SISTEMA OPERATIVO (LINUX RED HAT)

El sistema operativo más popular del mundo basado en código “Open Source”, el respaldo de la compañía líder mundial Red Hat le proporciona fiabilidad, flexibilidad, control, potencial y el soporte de millones de usuarios de la red. Esto es lo hace del sistema operativo Red Hat Linux la distribución más profesional y asequible, con reconocimiento internacional de toda la prensa empresas y usuarios.

Red Hat Linux Oficial es la mejor solución y la mas profesional tanto para estaciones de trabajo como para servidores basados en linux, gracias a sus miles de aplicaciones incluidas, y un sin número más disponibles atraves de la red y de los mayores y más profesionales de too el mundo, sistemas, fuentes, software, aplicaciones, paquetes integrados, juegos, documentación servicios entre otros todos está en Red Hat Linux.

Si pide una solución linux realmente profesional, más potencia a su sistema, más estabilidad a su software, mayor rapidez o total integración con internet, Red Hat Linux es la solución que busca. Este sistema operativo es de nueva generación, potente y muy estable, que ofrece un entorno de alto rendimiento tanto a servidores como estaciones de trabajo. Red Hat Linux, versión oficial, incluye miles de paquetes para todo tipo de usos, incluyendo internet, redes, entretenimiento, programación y desarrollo, gráficos, entre otros. Además Red Hat simplifica la instalación del software y su utilización a través de la tecnología RPM.

El código "Open Source" hace más veloz el desarrollo del software. Red Hat Linux versión oficial facilita el acceso a las últimas y mejores versiones. Desarrollado por una de las principales empresas que ofrece soporte técnico y las últimas novedades para Linux, Red Hat cuenta con toda una serie de ventajas y garantías sobre cualquier otra distribución Linux del mercado.

VENTAJAS DE RED HAT LINUX

- Control: Red Hat Linux le da el control porque incluye el código fuente. Ahora puede controlar la forma de trabajar del sistema y utilizar una nueva y flexible instalación seleccionando las interfaces de escritorio KDE o GNOME.

- Seguridad: Los servidores y las estaciones de trabajo que utiliza Red Hat Linux están preparados para funcionar durante meses, incluso años, sin reinicios con importantes mejoras en la disponibilidad de alta tecnología, consiguiendo siempre mejoras en la disponibilidad de alta tecnología, consiguiendo siempre mayores niveles de seguridad en los servicios de la red. Y si lo necesita tendrá el soporte telefónico para la instalación, y también a través de internet.

- Inversión: Para tener el sistema operativo Red Hat Linux no hay que pagar tasas por licencia. También puede ahorrarse los costes de la actualización

porque Red Hat Linux funciona eficazmente con Hardware antiguo. Red Hat incluye la mejor selección de aplicaciones “Open Source”: paquetes integrados, herramientas de productividad, desarrollo de aplicaciones, servidores para la red, correo electrónico, servidor internet, servidor de correos, sin costo adicional y sin largas descargas. Además Red Hat incluye, de forma exclusiva varios paquetes comerciales, juegos, versiones de demostración y ofertas de actualización de muchas aplicaciones y servicios.

CARACTERÍSTICAS PRINCIPALES DE RED HAT LINUX

- Herramientas de particionamiento y configuración del Firewall mejoradas durante el proceso de instalación.

- Administrador de ficheros Nautilus, integrando lectura de ficheros y de Web .

- Administración sencilla del sistema con herramientas graficas para configurar apache, usuarios y red.

- Configuración de red integrada: auto detección, auto configuración y soporte para modems, RDSI, xDSL y adaptadores de red.

- Auto detección del Hardware incluyendo los dispositivos USB, tarjetas gráficas, tarjetas de red y tarjetas de sonido.

- Soporte mejorado para portátiles; se habilita el soporte para PCMCIA por defecto y las herramientas de control del estado de la batería.

PAQUETES DE OFIMATICA STARTOFFICE

MEJORAS DEL KERNEL 2.4

- Sistemas de archivos Journaling ext3
- Aumenta del soporte para dispositivos

PARA LOS DESARROLLADORES

- Servidor de Web, de correo, ftp y de archivos
- Varios lenguajes de programación: C, C++, FORTRAN, Perl, Pitón, Tcl y CGI, PHP.
- Cadena de Herramientas de desarrollo actualizadas: gcc 2.96-RH, gdb 5.0, glibc 2.2.4.
- Herramientas de desarrollo para las aplicaciones de web PHP y mod_perl

4.1.2.2.- APACHE (SERVIDOR WEB)

Un Web Server es un software que permite poner a disposición de los Browsers páginas html, archivos y servicios que corren bajo el protocolo http, uno de los mejores ejemplos es Apache Web Server el cual lo hemos elegido por las siguientes características:

Apache es el servidor Web más usado en el mundo, un análisis realizado por Netcraft[1] en Marzo del 2002 presenta un 53.76% de dominios alrededor del mundo que utilizan Apache, para actualizar esta información visitar la dirección Web www.netcraft.net/survey/ aquí se puede visualizar el porcentaje actualizado de servidores Web Apache que están siendo utilizados en el mundo, este qeb server es Open Source, es decir, es gratis y permite realizar Virtual Hosting Apache normalmente se utiliza bajo sistemas Unix o Linux, pero existe un

[1] Proyecto cuyo objetivo es evaluar el uso de las herramientas utilizadas en los dominios de Internet

emulador para Windows, este emulador no se lo considera tan robusto como Apache de Unix, pero es muy recomendable para el desarrollo.

La página principal de Apache Web Project contiene todas las versiones de Apache con su respectiva documentación, usted puede bajar gratis e instalarlo o caso contrario en los discos de Instalación de Linux Red Hat vienen los instalables de Apache.

La dirección electrónica del Proyecto Apache es http://www.apache.org/.

4.1.2.3.- PHP (LENGUAJE DE PROGRAMACIÓN)

PHP es un lenguaje más utilizado alrededor del mundo que permite crear paginas Web dinámicas, además permite una codificación híbrida es decir permite utilizar varios lenguajes de programación para dar una gran solución Web, de esta manera podemos sacarle el mejor provecho a las características que cada lenguaje nos proporciona, al igual que Linux, PHP es Open Source, su sintaxis es muy parecida a C, Java, C++ lo que permite una breve adaptación a las personas que hayan programado en cualquiera de estos lenguajes. A PHP (Personal Home Page) se le conoce como procesador de hipertexto este nombre es muy bien puesto ya que el compilador de PHP preprocesa en el servidor Web la pagina PHP, y el resultado es HTML, de esta manera se convierte en un lenguaje de programación muy seguro, las características más importantes de PHP:

- Multiplataforma

  PHP se puede instalar casi en cualquier plataforma tales como Linux/Intel Linux/Alpha Compaq Tru64 Unix bajo sistema operativo Windows 9x/NT/Me/XP.

- Soporta múltiples bases de datos

PHP provee soporte para la mayoría de Bases de Datos Comerciales y freeware de las cuales podemos citar a MySQL, Oracle, Informix, Sybase, Postgresql entre otras el soporte es vía drivers nativos o ODBC.

– Soporta Varios protocolos e-mail

PHP es un lenguaje para desarrollo Web y queda por demás decir que maneja casi todos los protocolos de mensajería de Internet tales como: IMAP (Internet Message Access Protocol), POP3 (Post Office Protocol 3),SMTP (Simple Mail Protocol), USENET news protocol NNTP (Network News Transfer Protocol).

El sitio del PHP Project es www.php.net en este sitio se puede encontrar los instalables para varias plataformas, de la misma manera podemos encontrar el código fuente de PHP, y además los manuales de PHP en varios lenguajes y tipos de formato.

4.1.2.4.- SSL (CANAL SEGURO DE TRANSMISIÓN)

Un canal seguro de transmisión me permite encriptar toda la información que envían y reciben las máquinas que ha decidido establecer un canal seguro para la trasmitir de la información, SSL es una buena opción, rápida de adoptar y fácil de configurar.

Apache Web Server, con el módulo de seguridad mod_ssl y con las librerías del kit de herramientas OpenSSL son la combinación perfecta para poder configurar un servidor seguro, estos tres componentes son suministrados en las versiones de Red Hat Linux o se pueden encontrar las versiones más actualizadas en sus direcciones web.

Los Servidores Web suministran páginas Web a los navegadores que lo solicitan. En términos más técnicos, los servidores Web soportan el Protocolo de Transferencia de Hypertexto conocido como HTTP (HyperText Transfer Protocol),

el estándar de Internet para comunicaciones Web. Usando HTTP, un servidor Web envía páginas web en HTML y CGI, así como otros tipos de scripts a los navegadores o browsers cuando estos lo requieren. Cuando un usuario hace click sobre un enlace a una página Web, se envía una solicitud al servidor Web para localizar los datos nombrados por ese enlace. El servidor Web recibe esta solicitud y suministra los datos que le han sido solicitados (una página HTML, un script interactivo, una página web generada dinámicamente desde un base de datos, entre otros), o bien devuelve un mensaje de error.

El módulo mod_ssl es un módulo de seguridad para el Servidor Web Apache. El módulo mod_ssl usa las herramientas suministradas por el OpenSSL Project para añadir una característica muy importante al Apache. La posibilidad de encriptar las comunicaciones. A diferencia de las comunicaciones entre un navegador y un Servidor Web usando HTTP normal, se envía el texto íntegro, pudiendo ser interceptado y leído a lo largo del camino entre servidor y navegador.

El OpenSSL Project incluye un kit de herramientas que implementa los protocolos SSL y TLS (Transport Layer Security), así como una librería de codificación de propósito general, SSL se usa actualmente para la transmisión de datos segura sobre Internet. El protocolo TLS es un estándar de Internet para comunicaciones privadas y fiables sobre Internet. Las herramientas OpenSSL son usadas por el módulo mod_ssl para aportar seguridad en las comunicaciones Web.

Los discos de instalación de Linux Red Hat proveen todas estas herramientas para ser instalados ya sea al momento de instalar Linux o mas tarde, pero cada una de ellas tiene su propio proyecto donde se pueden encontrar las versiones más actuales, documentación y los parches.

El módulo de seguridad mod_sll es desarrollado por Ralf S, Engelshall se lo puede encontrar en www.modssl.org.

EL kit de herramientas OpenSSL, es desarrollado por Mark J Cox, Ralf S Engelschall, Dr Stephen Henson y Ben Laurie, se lo puede encontrar en www.openssl.org.

Software basado en el proyecto de servidor http Apache-SSL desarrollado por Ben Laurie se lo encuentra en www.apache-ssl.org.

4.1.2.5.- MIDGARD (SERVIDOR DE APLICACIONES)

Un Servidor de Aplicaciones ejecuta el software entre el navegador y los datos. Por ejemplo, cuando un cliente introduce un pedido desde un navegador Web, un servidor Web envía la solicitud al servidor de aplicaciones que ejecuta la lógica y también recupera y actualiza los datos del cliente desde las fuentes finales. El servidor de aplicaciones ejecuta los programas de negocio en lugar del cliente del Servidor Web o sistemas finales. Se sitúa entre un cliente y los datos empresariales y otras aplicaciones. Físicamente separa la lógica del negocio del cliente y los datos dentro de una arquitectura conocida como multi-capa. Los servidores de aplicaciones permiten a las empresas desarrollar y desplegar aplicaciones rápida y fácilmente e incrementan la cantidad de sus usuarios sin reprogramación.

4.1.2.6.- MYSQL (SERVIDOR DE BASE DE DATOS)

Mysql es una Base de Datos Freeware multi hilos además de tener características como el de ser una base de datos rápida, robusta y fácil de usar, éstas características la hacen tan popular, al mismo tiempo se sacrifican muchas otras características que Bases de Datos más serias si contemplan como es la integridad referencial, subselect, transacciones, triggers, procedimientos, entre otras. A MySQL se puede acceder directamente desde lenguajes tales como PHP, C, C++, Java y Perl vía drivers nativos.

La Base de Datos tanto los instalables como los fuentes podemos encontrarlos en www.mysql.com además es este sitio existen algunos programas de administración visual de MySQL, Tutoriales, ODBC, entre otros.

4.1.3.- COMUNICACIONES

Las comunicaciones que brinda un ASP son un factor determinante, para poder atraer a los clientes, ellos se sentirán satisfechos si tienen gran disponibilidad, que les permitan trabajar como si la aplicación estuviera instalada es su propio equipo, básicamente un ASP contrata los servicios de por lo menos dos ISP que le brinde una gran disponibilidad y rapidez.

4.1.3.1.- CONEXIÓN CON EL ISP (PROVEEDOR DE SERVICIOS DE INTERNET)

Los ISP proveedores de Internet son las empresas que proveerán el servicio de Internet, un ASP trabaja muy ligado a un ISP puesto que la idea principal es permitir proveer la aplicación vía Internet, los ISP que se contraten deben brindar gran flexibilidad puesto que el ASP puede variar el número de clientes en cualquier momento, el ISP debe proveerle la velocidad y ancho de banda suficiente para satisfacer a sus clientes.

TABLA IV.1 PROVEEDORES DE INTERNET Y TIPOS DE ENLACES QUE OFRECEN

PROVEEDOR	TIPO ENLACE	ANCHO DE BANDA	COSTO /MES
ANDINANET	DIAL UP		24 USD
ONNET	DIAL UP		22 USD
ECUADOR ON LINE	DIAL UP		25 USD
ESPOLTEL	DIAL UP		23.52 USD
HOY NET	WINGATE /12 USR		150 USD

HOY NET	LINEA DEDICADA	32 K	350USD
HOY NET	LINEA DEDICADA	64 K	500 USD
INTERACTIVE	DIAL UP		21 USD
ECUAFAST	LINEA DEDICADA	64 K	400 USD
ECUAFAST	LINEA DEDICADA	128 K	800 USD
TELCONET	DIAL UP		25 USD

Las tarifas aquí presentadas fueron obtenidas del web sites de las empresas a la fecha 10/07/2002

4.1.3.2.- MGETTY CONEXIÓN DIAL UP

Permite establecer una comunicación entre computadores vía modem, por medio de este tipo de conexión además de ser una manera muy barata de mantener la disponibilidad en el ASP si por alguna razón no se puede acceder a la aplicación mediante los ISP contratados.

4.1.4.- SEGURIDAD

La seguridad es una de las características más importantes que los ASP deben de tener en cuenta, ya que las aplicaciones estarán corriendo sobre Internet y mucha información que envíen a través de ellas es de carácter personal o secreto hoy en día contamos con algoritmos de encriptación muy avanzados que son muy difíciles de descubrir, aunque esta es una técnica muy antigua es la más utilizada y la que mejores resultados a generado, como ya hemos visto anteriormente utilizaremos SSL para proteger los datos además de configurar de manera muy cuidadosa los servidores y los servicios que estos brinden.

4.1.4.1.- FIREWALL

No hace mucho tiempo una red de cómputo era algo que no muchas empresas o escuelas tenían en su centro de cómputo. La gran mayoría de estas computadoras se encontraban aisladas una de la otra aunque se encontraran en

el mismo cuarto o salón de cómputo, únicamente grandes empresas, Instituciones Gubernamentales o Universidades tenían este recurso. Eso a cambiado con el paso del tiempo y hoy en día es común encontrar computadoras conectadas a una red y obtener información de ella o brindar servicios tal es el caso de Internet o una Intranet en una oficina u hogar, y es común el uso de ellas, como por ejemplo enviar y recibir correo electrónico, entre muchos servicios más.

El gran desarrollo de estas redes no ha sido del todo positivo en varios aspectos. Uno de ellos es la disponibilidad de Direcciones IP, que esta limitado a 4.300 millones de direcciones IP validas aproximadamente. Esta cantidad de direcciones puede ser a primera vista muchísimas direcciones, pero direcciones validas libres en Internet son actualmente muy pocas, por lo que cada vez es más difícil poder obtener una dirección valida en Internet. Con la llegada de la versión 6 del protocolo IP se espera poder extender este rango de direcciones en un par de millones más. Pero como esta nueva versión aun no se encuentra disponible debemos de trabajar con la actual (IPv4) y por ende debemos administrar mejor el uso de este tipo de direcciones. Una forma de administrar mejor esto, es escondiendo computadoras con direcciones no validas dentro de una red, detrás de una dirección IP valida. A esta técnica se le conoce como enmascaramiento de direcciones. Existe otro problema que no es técnico sino social. Cada día existen más computadoras y personas que accesan a Internet. La necesidad de proteger los sistemas conectados a una red de usuarios no deseados es cada vez más común y se vuelve más importante día a día.

Instalar un Firewall es una buena solución para protegerse de ataques a una red interna o de usuarios no deseados. Actualmente, el Kernel de Linux RedHat soporta filtrado de paquetes, que pueden se utilizados para implementar un sencillo Firewall.

4.2.- CONFIGURACIÓN DE PROTOTIPO OPERATIVO DE UN ASP

En esta sección se establecerá el diseño de la red interna del ASP, además de los comandos que han de ejecutarse y los scripts que deben ser modificados para poder configurar un Servidor Web, un Servidor de Aplicaciones, un Servidor de Base de Datos, un Firewall conexiones Dial-Up.

También se proporciona los scripts modificados en el disco bajo la carpeta configuración .

4.2.1.- HARDWARE

En las siguientes líneas se presenta los requerimientos mínimos de hardware necesarios para poner en funcionamiento un ASP, esto se ilustra en la figura de la arquitectura básica de un ASP.

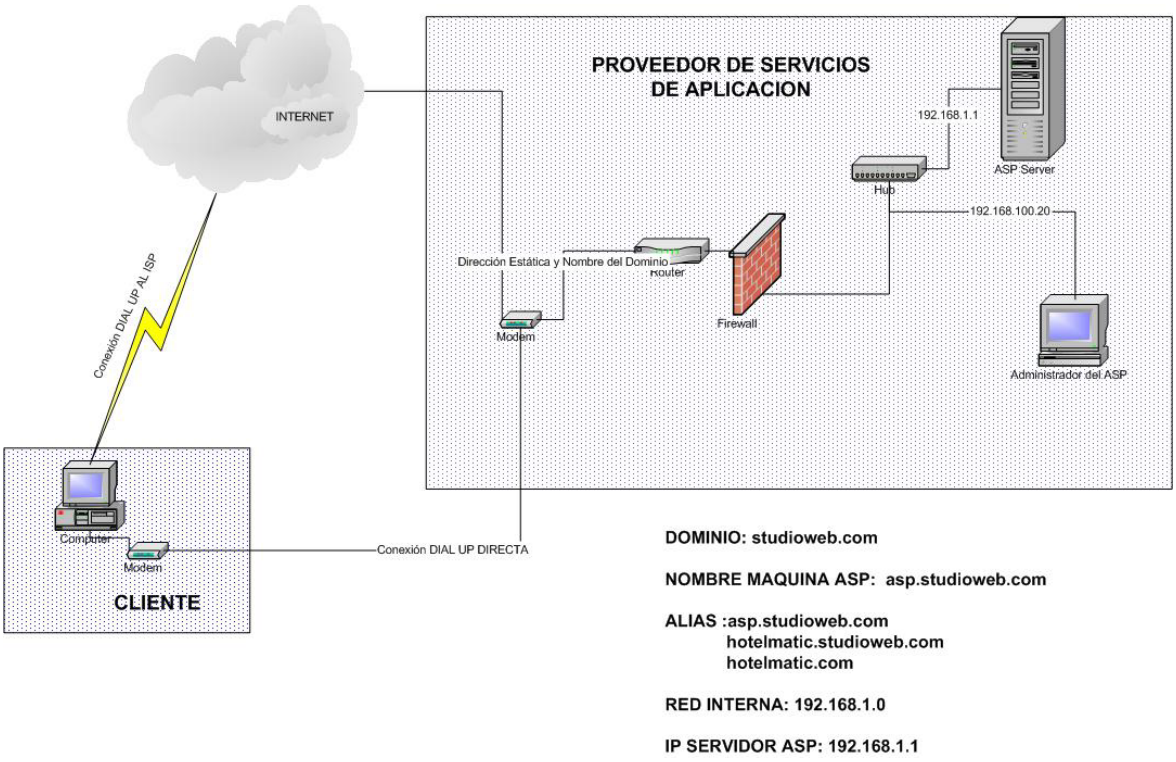
TABLA IV.2 REQUERIMIENTOS DE HARDWARE PARA LA IMPLEMENTACIÓN DE UN PROTOTIPO OPERATIVO

HARDWARE	CARACTERISTICA	CANTIDAD
Computador PC	Pentium III	1
PC Administrador	Pentium III	1
Hubs	Hub 3COM 16 puertos 10/100	1
BackUps	CD-RWRITER	1

4.2.1.1.- CONFIGURACIÓN DE LA RED INTERNA DEL ASP

En el siguiente gráfico se presenta la red que se ha configurado para el prototipo operativo del ASP.

FIGURA 4-1 RED DEL ASP



4.2.2.- SOFTWARE

El software viene incluido en los discos de Instalación de Linux RedHat, es un software Freeware, de la igual manera cada paquete tiene su propia dirección Web en la cual se puede encontrar las versiones más actualizadas, la documentación requerida para su instalación y configuración en esta sección se hará referencia a cada paquete que debemos instalar además la manera básica de configuración.

4.2.2.1.- DNS

Un servidor DNS (servidor de nombre de dominio) debe ser configurado, puesto que de esta manera podremos especificar el nombre y los alias del servidor web, talvés lo más difícil de un servidor es manejar correctamente la parte del DNS, es por esto que desde el punto de vista técnico, si no esta bien configurado el DNS, la red siempre tendrá problemas. Cuando un DNS está correctamente configurado se pueden hacer trucos inclusive de ruteo simplemente cambiando las definiciones de las tablas. Los DNS pueden ser primarios o secundario dependiendo de la configuración que se haya elegido para el mismo, y está en la capacidad de administrar más dominios de clientes que a futuro pretendan hacer Web Hosting o ver –email.

La definición en el Linux está en /etc, y al final dos archivos se copian a /var/named/ para que cuando el servidor suba su DNS saque la definición de ellos. Los archivos que se van tocando en orden son los siguientes:

4.2.2.1.1.- CONFIGURACION DEL DNS

Archivo /etc/named.conf

```
//Se debe aumentar la zonas primarias y reversas según sea el caso
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "named.1.168.192";
        allow-update { none; };
};
zone "studioweb.com" IN {
        type master;
        file "named.studioweb.com";
        allow-update { none; };
};
```

Archivo /var/named/named.studioweb.com

```
$TTL  86400
@ IN    SOA    studioweb.com. root.studioweb.com.  (
                        2001030300 ; Serial
                        28800     ; Refresh
                        14400     ; Retry
                        3600000    ; Expire
                        86400 )    ; Minimum
          NS     ns
             MX     10 mail

localhost      A      127.0.0.1
ns             A      192.168.1.1
mail           A      192.168.1.1
www            A      192.168.1.1
ftp            A      192.168.1.1
webmail        A      192.168.1.1
```

Archivo /var/named/named.1.168.192

```
$TTL  86400
@      IN     SOA    studioweb.com. root.studioweb.com.  (
                        2001030300 ; Serial
                        28800     ; Refresh
                        14400     ; Retry
                        3600000    ; Expire
                        86400 )    ; Minimum
          NS     omnisoftcorp.net.
             MX     10 mail.omnisoftcorp.net.

1              PTR    studioweb.com.
1              PTR    mail.studioweb.com.
1              PTR    www.studioweb.com.
1              PTR    ftp.studioweb.com.
```

1 PTR webmail.studioweb.com.

4.2.2.2.- APACHE

La instalación de un Apache Web Server, se la puede realizar de dos maneras la primera en el momento de instalar Linux o la segunda cuando ya se haya instalado, aunque es recomendable la primera por su facilidad; cuando ya tenemos instalado Linux y deseamos subir el servicio de Web Server debemos seguir los siguientes pasos, *cabe resaltar que esta es una breve descripción de la instalación, si queremos conocer más al detalle se debe referir al sitio web* www.apache.org *o a la documentación de Linux.*

4.2.2.2.1.- PASOS PARA LA INSTALACIÓN Y CONFIGURACIÓN DE APACHE WEB SERVER

1. Obtener la última versión de Apache del sitio web
2. Copiar el paquete a un directorio en Linux por ejemplo al **/usr/src**
3. Cambiar de directorio donde se encuentra el paquete
   # cd /usr/src
4. Descomprimir el paquete
   # tar zxvf apache-1.3.20-16.tar.gz
5. Cambiar de directorio en el cual descomprimimos apache
   #cd apache-1.3.20-16/
6. Ejecutamos el comando de configuración de esta manera hemos concluido la instalación de Apache
   #./configure –prefix=/usr/local/apache
7. Para configurar apache debemos buscar el archivo de configuración de Apache ***httpd.conf*** en el cual debemos configurar algunas de directivas:

   – ServerType

Puede estar configurado como inetd o standalone. Por defecto Red Hat esta configurado como standalone, esto significa que el servidor arranca una vez y el servidor maneja todas las conexiones, cuando esta configurado como inetd significa que para cada conexión HTTP, crea una instancia nueva de servidor, cada instancia de servidor gestiona la conexión y termina al terminar la conexión. Como se puede imaginar, utiliza inetd es muy ineficiente, por tal razón a la directiva se la debe dejar como sigue:

ServerType standalone.

- TimeOut

  Define en segundos el tiempo que el servidor esperará para recibir y enviar peticiones durante la comunicación. Específicamente TimeOut define cuanto esperará el servidor a recibir peticiones GET, cuanto esperará a recibir paquetes TCP en una petición POST o PUT. TimeOut está puesto a 300 apropiado para la mayoría de las situaciones.

  Time Out 300

- MaxClients

  Establece un límite de clientes que podrán conectarse concurrentemente al Web Server, en esta ocasión para nuestro ASP se debe de tener en cuenta el número de clientes y basándose en ello establecer esta directiva, la razón principal de tener el parámetro MaxClients es evitar que un servidor errático vuelva inestable al sistema operativo.

  MaxClients 125

- DocumentRoot

  Es el directorio que contiene la mayoría de los archivos HTML que se entregan en respuesta a peticiones, por defecto el DocumentRoot

para un servidor seguro y no-seguro es **/var/www/html**, aunque no es muy recomendable el dejar este valor por defecto por que los intrusos ya saben de antemano en cual directorio buscar los archivos, lo recomendable es cambiar por cualquier directorio que el administrador decida.
DocumentRoot /var/www/html

- DirectoryIndex

Es la página por defecto entregada por el servidor cuando hay una petición de índice de un directorio especificando una barra al final del nombre del directorio, por ejemplo cuando un usuario pide la página http://www.yahoo.com/ van a recibir la página DirectoryIndex si existe o un listado generado por el servidor. El valor por defecto para DirectoryIndex es index.html index.htm index.php index.php3 index.phtml index.shtml index.cgi, el servidor intentará encontrar cualquiera de estos cuatro y entregará el primero que encuentre, si no encuentra ninguno y si Options Indexes está puesto para el directorio, el servidor generará un listado en formato HTML de los subdirectorios y archivos del directorio.

- ServerAdmin

En esta directiva se la debe configurar preferiblemente con la dirección mail del webmaster o administrador del sistema pues si ocurre algún error con Apache éste enviará un mail a la dirección indicando, por ejemplo:
webmaster@studioweb.com

- ServerName

Esta directiva me especifica el nombre del dominio de mi Web Server debe ser un DNS (Domain Name Service) válido que se tenga derecho de usar no basta con inventarse algo, por ejemplo.
ServerName localhost

8. Directivas para iniciar para o reiniciar Apache
   - Iniciar
     # service httpd start
   - Parar
     # service httpd stop
   - Reiniciar
     # service httpd restart

Además *# service httpd reload* me permite actualizar Apache si ha cambiado alguna de las directivas del archivo httpd.conf sin parar el servicio.

4.2.2.3.- SSL (MODULOS DE SEGUIDAD)

Si ha instalado Red Hat Linux sin los paquetes relacionados con la seguridad del servidor, y un tiempo después decide que quiere instalar un servidor seguro, lo que podrá hacer. La manera más fácil de llevarlo a cabo es usar RPM Genome-RPM o Kpackage para instalar los paquetes RPM incluidos en el CD de Red Hat Linux.

Antes de proceder a instalar los módulos de seguridad se debe parar el servidor Web si se esta ejecutando, y los pasos son los siguientes:

1. Montar el CDROM
   Para empezar el proceso de instalación, deberá montar el CDROM primero, sitúe apropiadamente el CD de RedHat Linux en la unidad de CDROM, cambie a usuario root y teclee el comando siguiente para montar el CD.

#mount /mnt/cdrom

Si por alguna razón obtiene un mensaje de error después del comando, pruebe con:

#mount –t iso9660 /dev/cdrom /mnt/cdrom

2. Instalación de paquetes

Una vez que montado el CDROM instalamos los paquetes **apache, openssl y mod_ssl** con el siguiente línea de comandos.

Para instalar apache

#rpm –Uvh apache-1.3.20-16.i386.rpm

Para instalar openssl

#rpm –Uvh openssl-0.9.6b-8.i386.rpm

Para instalar mod_ssl

#rpm –Uvh mod_ssl-2.8.4-9.i386.rpm

Si existe algún error podemos utilizar –f como parámetro para forzar la instalación

4.2.2.3.1.- CREANDO UN CERTIFICADO SELF-SIGNED

Puede crear su propio certificado self-signed, pero note que este certificado no proporciona la garantía de seguridad proporcionada por un certificado CA, si quiere hacer su propio certificado self-signed, primero necesita crear una clave aleatoria usando los siguientes pasos:

1. Primero necesita eliminar las claves y certificados que fueron generados durante la instalación cd al directorio /etc/httpd/conf y usamos el comando para borrar dos archivos
   #rm ssl.key/server.key
   #rm ssl.crt/server.crt

2. Crear una propia clave aleatoria, teclee el siguiente comando
   make genkey
   su sistema mostrará un mensaje similar al siguiente:
   Enter PEM pass phase:

   Aquí debe introducir el password por razones seguridad debe ser mayor de 8 caracteres, tener números y signos de puntuación, cuando presiones enter tendremos que introducir nuevamente el password por efectos de verificación, además debemos recordar esta clave ya que se nos preguntará cada vez que se levante el servidor Apache, en este momento se ha creado un archivo server.key que contiene la clave, por supuesto este archivo esta encriptado.

   Luego de tener generada la clave aleatoria se utiliza el siguiente comando.
   make testcert
   Se creara un archivo que es inducido de su password, en este momento se le pedirá que ingrese su password y luego se le preguntará por alguna información que deberá llenar, después de proporcionar la información correcta un certificado self-signed será creado y colocado en /etc/httpd/conf/ssl.crt/server.crt, necesitará reiniciar su servidor seguro después de generar el certificado.

4.2.2.3.2.- COMPROBANDO SU CERTIFICADO

Cuando se ejecuta el servidor Apache seguro se le preguntará por el password que uso para general la clave y luego Apache se ejecutará, para comprobar su certificado usted debe de abrir el browser puede ser mozilla y el en URL poner la

dirección de su servidor web, su servidor web le mostrará una caja de dialogo indicándole que su browser debe ser configurado para aceptar el certificado comprobado, en ese momento podrás ver que en el URL en el prefijo aparece https es decir HTTP en modo seguro, además podrás ver un candado cerrado si estas utilizando Internet Explorer o una llave completa si utilizas Netscape.

4.2.2.4.- MYSQL (SERVIDOR DE BASE DE DATOS)

Para instalar MySQL se requieren de los siguientes pasos:

1. Obtener los paquetes de las versiones más actualizadas del proyecto MySQL cuya dirección web oficial es www.mysql.com
   Grave el archivo en un directorio conveniente por convención se utiliza /usr/src para guardar los fuentes.

2. Cambio de directorio a
   #cd /usr/src

3. Instalar el paquete
   #rpm –ivh mysql-server-3.23.41-1.i386.rpm

De esta manera hemos instalado MySQL luego de la instalación de Linux si deseamos ejecutar MySQL entonces en la línea de comandos tecleamos.

#safe_mysqld &

El (&) me indica que este proceso se estará ejecutando en background
Para establecer el usuario y password debemos ejecutar el siguiente comando.

#mysqladmin –u root password “nuevo password”

En la versión actual de Apache ya viene instalados los drivers para manejar MySQL por defecto así que no debemos levantar ningún módulo.

4.2.2.5.- PHP (COMPILADOR)

Para instalar PHP debemos obtener las versiones más actualizadas de PHP hoy tenemos la versión 4 no es muy difícil como ya hemos visto se obtiene los RPM desde la dirección web oficial del proyecto www.php.net y se instala, ya en la versión de PHP4 no se necesita configurar nada en Apache para indicarle que debe compilar PHP este ya está configurado por defecto el comando para instalar PHP es:

#rpm –ivh php-4.0.6-7.i386.rpm

4.2.2.6.- MIDGARD (SERVIDOR DE APLICACIONES)

Lo primero que ha que hacer es dirigirse a www.midgard-project.com y bajarse la ultima versión de este paquete.

Pasos para la instalación

Una vez obtenidos todos los archivos de midgard para esta ocación son 5 se los procede a descomprimir.

Instalación de la Librería de Midgard

 # cd midgard-lib-1.4 (directorio que contiene los instalables de la librería)
 # ./configure –with-apxs=/usr/sbin/apxs
 # make

 # make install

Para Linux Red Hat se debe editar el archivo **/etc/ld.so.conf** y aumentar las siguientes lineas:

/usr/local/midgard/lib

/usr/local/lib

Para actualizar el archivo que acaba de editar corra en siguiente comando.

 # /sbin/ldconfig

Instalación de la Base de Datos de Midgard

 # cd midgard-data-1.4

 # ./configure --with-apxs=/usr/sbin/apxs

 # ./dbinstall

Módulo de Midgard para Apache

 # cd mod_midgard-1.4

 # ./configure –with-midgard=/usr/sbin/apxs

 # make

 # make install

Instación de Midgard PHP4

 # cd midgard-php-1.4

 # ./configure –with-apxs=/usr/sbin/apxs –with-midgard=/usr/local/midgard

 # make

 # make install

Editar el Archivo de Configuración Apache (httpd.conf)

Al final del archivo **httpd.conf** se debe añadir la siguiente línea

Include /usr/src/midgard/midgard-data-1.4.3/midgard-data.conf

Si el archivo **midgard-data.conf** se encuentra en otro path habrá que redireccionarlo

4.2.2.7.- MGETTY CONEXIÓN DIAL UP

Mediante la configuración de mgetty, nuestros clientes podrán conectarse directamente con el ASP sin necesidad de utilizar un ISP, o en la posible eventualidad que los ISP contratados se encuentren fuera de servicio, para poder recibir llamadas, obviamente debemos tener un modem conectado a un puerto serie, soporte en el kernel, directamente incluido o como módulo, para el protocolo PPP, así como los paquetes pppd y mgetty+sendfax, para la configuración se necesita configurar varios scripts que a continuación detallamos.

1.- **/etc/mgetty+sendfax/mgetty.config**

port ttyS0
debug 9
speed 57600
#Acepta solo datos
data-only yes
init –chat “” \d+++\dAT&FH0 OK
#Números de rings antes de que mgetty descuelgue
rings 1

2.- **/etc/mgetty+sendfax/login.config**

/AutoPPP/ -- /usr/sbin/pppd file /etc/ppp/options.server

3.- **/etc/ppp/options.server**

debug
modem
crtscts
/dev/ttyS0
57600
asyncmap 0
#Requiere autentificación
auth
#Se va a utilizar el archivo de password /etc/passwd o /etc/shadow
login
#Dirección IP asignada al ordenador remoto
:192.168.100.200
proxyarp
nodetach
refuse-chap
require-pap
#Dirección IP del Servidor DNS que le será entregado al cliente Windows
ms-dns 192.168.100.1

4.- **/etc/ppp/pap-secrets**

#Autentificación usando PAP

#cliente	*servidor*	*secret*	*IP Dirección*
*	*	“”	*192.168.1.200*

5.- **/etc/inittab/**

S0:2345:respawn:/sbin/mgetty /dev/ttyS0

6.- **Para que se actualice los cambios usar el siguiente comando**

#init q

4.2.2.8.- FIREWALL

Un Firewall es un mecanismo diseñado para prevenir el acceso no autorizado hacia su red privada. Un Firewall típicamente actúa como un GATEWAY, que es

una computadora en la cual acceden siempre la primera vez que alguien ingresa a su red. Por tanto, toda la actividad defensiva debe proporcionarla el Gateway, y que algunas veces es llamado "Bastion host“, que por su nombre hace referencia a los bastiones que eran los puntos crítios donde se concentraban las defensas de los castillos medievales.

Para la configuración de un Firewall debemos de tener en cuenta a que redes vamos a dar acceso y a que redes no vamos a denegar el acceso para eso se crean reglas que en nuestro caso son las siguientes.

Para permitir que los usuarios de mi red puedan navegar en el Internet, lo más fácil y recomendable es enmascarar los paquetes; con la siguiente línea de comando permito que la red 192.168.1.0/24 enmascare los paquetes y puedan todas las máquinas que están en esta red navegar.

#ipchains –A forward –p tcp –I ppp0 –s 192.168.1.0/24 –d 0.0.0.0/0 –j MASQ

Capitulo

5

V.- DESARROLLO DEL SISTEMA HOTELMATIC

El presente capítulo hace referencia al proceso de desarrollo de Software que se ha de seguido para el análisis, diseño, y construcción del Sistema Hotelero, en primera instancia se encuentran los requisitos de Software que debe satisfacer el sistema, ya en puntos posteriores se tratará a UML como metodología para establecer el análisis y diseño .

5.1.- ESPECIFICACION DE REQUISITOS DE SOFTWARE

En el preste documento se describe la especificación de requisitos de Software basado en el estándar IEEE/830.

5.1.1.- INTRODUCCION

El siguiente documento se especifican los Requisitos de Software para el sistema hotelero, todo su contenido ha sido realizado en base a un estudio realizado con sistemas similares y varios administradores de hoteles, esta especificación ha sido realizada adoptando el estándar de la Especifica de Requisitos de Software 830/1998 ANSI/IEEE.

5.1.2.- PROPOSITO

El objetivo de este documento es definir de manera clara y precisa todas las funcionalidades y restricciones del sistema, este documento va dirigido al desarrollador y usuarios finales del sistema.

5.1.3.- AMBITO DEL SISTEMA

En primera instancia y para el tema de estudio que se está tratando el sistema servirá de ejemplo para implantarlo en el ASP pero en el futuro el objetivo es crear una red hotelera que permita enlazar las agencias de turismo con los hoteles y hostales, de tal manera que las agencias de turismo cuenten con la información de disponibilidad, ocupación de las habitaciones y servicios ofrecidos por los hoteles, este sistema será totalmente diseñado y codificado con herramientas Open Source e Implementado en Ambiente Web.

5.1.4.- DEFINICION DE ACRONIMOS Y ABREVIATURAS

En esta sección se definirán todos los términos, acrónimos y abreviaturas utilizadas en la ERS.

5.1.4.1.- DEFINICIONES

TABLA V.1 TABLA DE DEFINICIONES

Operario	Persona encargada de las operaciones de un Hotel
Administrador	Persona encargada de la Administración de un Hotel
Clientes	Persona que realiza reservaciones o se hospeda en un Hotel
Hoteles, Hostales y Hosterias	Lugares en los cuales la gente reserva y utiliza habitaciones durante un cierto tiempo además de realizar consumos y llamadas telefónicas

5.1.4.2.- ACRONIMOS

TABLA V.2 TABLA DE ACRÓNIMOS

ERS	Especificación de Requisitos de Software
OEM	Open Equipment Manufacturer
PBX	Centro de Comunicaciones

5.1.4.3.- ABREVIATURAS

TABLA V.3 TABLA DE ABREVIATURAS

HOTELMATIC	Sistema Hotelero
OMNISOFT	Empresa ecuatoriana desarrolladora de software orientado al Internet
CHECK IN	Registro de Ingreso de Clientes
CHECK OUT	Registro de Salida de Clientes

5.1.5.- REFERENCIAS

Estándar ANSI/IEEE de Especificación de Requisitos de Software 830/1998.

5.1.6.- DESCRIPCION GENERAL

En esta sección se presentan una descripción a alto nivel del sistema. Se encuentran las principales áreas de negocio a las cuales el sistema debe dar soporte, las funciones que el sistema debe realizar, la información utilizada, las restricciones y otros factores que afecten al desarrollo del mismo.

5.1.6.1.- PERSPECTIVA DEL PRODUCTO

EL sistema actualmente servirá para verificar el buen funcionamiento del ASP pero la proyección es crear una Red Virtual Hotelera cuyo objetivo es enlazar las agencias de turismo con los hoteles, hostales, además los hoteles que

pertenezcan a esta red, tendrán como beneficio la colocación y promoción de sus servicios.

5.1.6.2.- FUNCIONES DEL SISTEMA

Las siguientes funciones que a continuación se describen son vitales para el buen funcionamiento del sistema Hotelero.

- Módulo de la Administración del Hotel:

En la administración del sistema se va a tener en cuenta la creación de usuarios, el registro centro de costos, el registro de gastos, el registro de habitaciones, para el registro de habitaciones se debe de tener en cuenta la disponibilidad y la temporada, por que bajo este factor el costo de las habitaciones aumentará en un porcentaje, el sistema debe permitir parametrizar este valor.

- Módulo de Operaciones del Hotel:

Las operaciones básicas en el hotel son las reservaciones de las habitaciones, el registro de ingreso de clientes, el registro de salida de clientes del hotel, el registro de consumos, y llamadas telefónicas.

Cuando una persona realiza una reservación se debe tener en cuenta la disponibilidad de las habitaciones de la misma manera el cliente podrá conocer el precio por la reservación de la habitación
Cuando los clientes llegan al hotel cada uno debe Gestionarse y llenar su hoja de registro, solamente los clientes que hayan sido registrados pueden hacer consumos o llamadas telefónicas, una vez terminada la reservación se debe realizar el registro de salida del cliente.

5.1.6.2.1.- GESTION DE USUARIOS

El sistema debe aceptar dos tipos de usuarios el Administrador y Operador, cada ves que se desee Gestionar un nuevo usuario se requiere la siguiente información: Tipo de Usuario, código de usuario este será único para cada usuario y es de responsabilidad de la persona que utilice el sistema este código, el usuario usará para ingresar a sistema, también se necesita una clave de usuario, de los datos de usuarios esenciales se necesita el nombre, apellido, cargo, departamento, dirección, teléfono, fax, e-mail, fotografía del usuario, y el sueldo .

5.1.6.2.2.- GESTION DE CENTRO DE COSTOS

Se necesita Gestionar los centros de costos que utilizara el Hotel en base al centro de costos se obtendrán los ingresos y egresos realizados por el Hotel, para cada centro de costos se requiere la siguiente información un código, el nombre y una descripción del centro de costo.

5.1.6.2.3.- GESTION DE HABITACIONES

El sistema permitir Gestionar habitaciones y se debe tener en cuenta la siguiente información, código de la habitación, piso en la cual se encuentra la habitación, estado, tipo, tarifa, y es necesario que se registre una fotografía de la habitación

Luego de Gestionar una habitación será imperante Gestionar el porcentaje de incremento en el valor de la habitación, este aumento dependerá de la temporada en la cual se encuentre, existen tres tipo de temporada (alta, media, baja) cada temporada se Gestionar con su respectiva fecha de inicio y finalización.

5.1.6.2.4.- GESTION DE TARIFAS TELEFÓNICAS

El sistema debe permitir Gestionar diferentes servicios telefónicos que brinda a los clientes, tales como conexión a Internet, llamadas nacionales regionales o locales, llamadas internacionales entre otros servicios de telefonía que los hoteles brindan.

5.1.6.2.5- GESTION DE RESERVACIONES

Cuando se realice una reservación se debe de tener en cuenta la disponibilidad de habitaciones, para el registro de la reserva se requiere la siguiente información: el código de la reservación, nombre, apellido, dirección, teléfono, del cliente, la fecha de inicio y fecha de finalización de la reserva, el número de adultos, el numero de menores de edad, la tarifa, el tipo de reserva, fecha máxima en la cual se puede confirmar la reserva, además ocasionalmente algunas veces se necesita alguna observación con respecto a la reservación.

En este proceso se debe de realizar la asignación de habitaciones a la reservación, cuando una reservación no se ha llegado a concretar el sistema automáticamente debe liberar las habitaciones y ponerlas a disposición para otros clientes.

5.1.6.2.6.- GESTION DE INGRESO DE CLIENTES (CHECK IN)

Al proceso de registro de ingreso de clientes en el Hotel, se le conoce como CHECK IN para esto se requiere de la siguiente información, código del registro, nombre, apellido, fecha de nacimiento, nacionalidad, dirección, teléfono, fax, ciudad, país profesión, empresa, cargo, pasaporte estado civil, procedencia del cliente; se debe tener en cuenta que todos los clientes deben tener su registro de entrada.

5.1.6.2.7.- GESTION DE LLAMADAS TELEFONICAS

Solo los clientes registrados podrán realizar consumos de servicio telefónico ya sea conexión a Internet, llamadas nacionales locales o regionales, llamadas internacionales, entre otros, cada una de estas llamadas serán registradas con la siguiente información: Centro de Costos al que pertenece, código del cliente que realizo la llamada, fecha, duración y valor de la llamada.

5.1.6.2.8.- GESTION CONSUMOS

De la misma manera que el consumo de servicios telefónicos, solamente los clientes que estén registrados podrán realizar consumos, para el registro de los consumos se necesita la siguiente información: Centro de Costos, código del tipo de consumo, código del cliente que realiza el consumo, fecha, cantidad, forma de pago, pueden existir dos formas por tarjeta o en efectivo, si es por tarjeta hay que especificar el número de voucher.

5.1.6.2.9.- GESTION DE SALIDA DE CLIENTES (CHECK OUT)

Cuando ya haya terminado la reservación se debe Gestionar la salida del cliente en el contexto hotelero se le conoce como CHECK OUT, para lo cual se requiere que el cliente registre la siguiente información: fecha de registro de salida, forma de pago, destino, factura, numero de pasaporte o equivalente.

5.1.6.2.10.- GESTION DE GASTOS

El sistema debe permitir Gestionar los gastos que realiza el hotel cada gasto se realiza en base a un centro de costo, los datos requeridos para cada ingreso de gastos son los siguientes fecha, cantidad, valor, forma de pago, y una breve descripción del gasto.

5.1.6.2.11.- GESTION TIPOS DE SERVICIOS TELEFONICOS

El sistema permitirá Gestionar diferentes tipos de servicios telefónicos tales como conexión a Internet, Llamadas Internacionales, Llamadas regionales, para el ingreso se necesita que se registre la siguiente información tipo, tarifa, categoría, localidad, moneda.

5.1.6.2.12.- GESTION TIPOS DE GASTOS

El sistema permitirá Gestionar diferentes tipos gastos en los cuales incurre el hotel, tales como insumos de habitaciones, para el ingreso de cada tipo de gasto se necesita que se registra la siguiente información nombre, código, precio, descripción, moneda.

5.1.6.2.13.- GESTION TIPOS DE CONSUMOS

El sistema permitirá Gestionar diferentes tipos de consumos más comunes que el cliente realiza, de esta manera se podrá llevar un mejor control de los gastos por cada tipo, para Gestionar un nuevo tipo de consumo se necesita de que se registre la siguiente información: Código, Centro de Costos que pertenece, descripción precio y moneda.

5.1.6.3.- CARACTERÍSTICAS DE LOS USUARIOS

El sistema Hotelero debe ofrecer una interfaz de usuario intuitivo fácil de aprender y sencillo de manejar. El sistema debe presentar un grado alto de usabilidad, sería deseable que un usuario se familiarice en un máximo de 5 horas con el sistema.

Básicamente los usuarios del sistema serán administradores y empleados de hoteles que conocen como se realizan los procesos hoteleros, pero en cuestión de aplicaciones no tienen mucha experiencia de allí que el sistema debe presentar la mayor de las facilidades de aprendizaje.

5.1.6.4.- RESTRICCIONES

El sistema se realizará en base a un sistema anterior realizado por la empresa Omnisoft que según varios comentarios y experiencia de algunos administradores hoteleros o personas relacionadas con el tema de hoteles es muy bueno, realmente este sistema tiene las funcionalidades generales comunes que todos los hoteles u hosterías manejan.

Dentro de lo que no esta considerado es:

- El sistema no facturará
- No se comunicará con otros sistemas
- Trabajará independientemente y no tendrá interfaces con servicios tales como e-mail, chat entre otros

En cuanto a las restricciones de Hardware y Software, la empresa exige que el sistema funcione en ambiente Web y utilice como lenguaje de programación PHP y como base de datos MySQL.

5.1.6.5.- SUPOSICIONES Y DEPENDENCIAS

En esta sección se encuentran todas las suposiciones, dependencias con otros sistemas.

5.1.6.5.1.- SUPOSICIONES

Se asumes que los requisitos ya han sido previamente analizados y aprobados cualquier modificación debe ser aprobada por todas las partes involucradas y se

debe actualizar este documento ya que en base a este se desarrollara el sistema hotelero.

5.1.6.5.2.- DEPENDENCIAS

Hotelmatic funciona autónomamente, sin necesidades de comunicarse con otros sistemas externos, por lo que no hay dependencia respecto a otros sistemas.

El sistema seguirá una arquitectura de por lo menos tres capas físicas y lógicas, por lo que la disponibilidad del sistema dependerá mas de la conexión con el ISP, de no poder hacerlo mediante un ISP se podrá realizar directamente conectándose a la PBX del ASP.

5.1.7.- REQUISITOS ESPECIFICOS

En la siguiente sección se especifican los requisitos a un nivel de detalle suficiente para que se permita realice un buen diseño, realizar el análisis de requisitos que demuestre que el sistema satisface o no, los requisitos.

5.1.7.1.- REQUISITOS FUNCIONALES

En las siguientes líneas se especifican los requisitos a un mayor detalle permitiendo un mejor entendimiento del sistema.

5.1.7.1.1.- GESTION DE USUARIOS

- El sistema deberá permitir:
- Req(01) Ingresar un nuevo Usuario
- Req(02) Eliminar un Usuario
- Req(03) Modificar los datos de un Usuario
- Req(04) Consultar en forma individual los datos de un Usuario del sistema

5.1.7.1.2.- GESTION DE CENTRO DE COSTOS

- El sistema deberá permitir:
- Req(06) Ingresar un nuevo Centro de Costo
- Req(07) Eliminar un Centro de Costo
- Req(08) Modificar los datos de un Centro de Costo
- Req(08) Consultar en forma individual los datos de un Centro de Costo

5.1.7.1.3.- GESTION DE HABITACIONES

- El sistema deberá permitir:
- Req(10) Ingresar una nueva Habitación
- Req(11) Eliminar una Habitación
- Req(12) Modificar los datos de una Habitación
- Req(13) Consultar en forma individual los datos de una Habitación

5.1.7.1.4.- GESTION DE TARIFAS TELEFÓNICAS

- El sistema deberá permitir:
- Req(14) Ingresar una nueva Tarifa Telefónica
- Req(15) Eliminar una Tarifa Telefónica
- Req(16) Modificar los datos de una Tarifa Telefónica
- Req(17) Consultar en forma individual los datos de una Tarifa Telefónica

5.1.7.1.5- GESTION DE RESERVACIONES

- El sistema deberá permitir:
- Req(18) Ingresar una nueva Reservación
- Req(19) Eliminar una Reservación
- Req(20) Modificar los datos de una Reservación

– Req(21) Consultar en forma individual los datos de una Reservación

5.1.7.1.6.- GESTION DE INGRESO DE CLIENTES (CHECK IN)

– El sistema deberá permitir:
– Req(22) Ingresar un nuevo Cliente
– Req(23) Eliminar un Cliente
– Req(24) Modificar los datos de un Cliente
– Req(25) Consultar en forma individual los datos de un Cliente

5.1.7.1.7.- GESTION DE LLAMADAS TELEFONICAS

– El sistema deberá permitir:
– Req(26) Ingresar el consumo de una nueva llamada telefónica
– Req(27) Eliminar el consumo de una llamada telefónica
– Req(28) Modificar los datos del consumo de una llamada telefónica
– Req(29) Consultar en forma individual los datos del consumo de llamada telefónica

5.1.7.1.8.- GESTION CONSUMOS

– El sistema deberá permitir:
– Req(30) Ingresar un nuevo Consumo
– Req(31) Eliminar un Consumo
– Req(32) Modificar los datos de un Consumo
– Req(33) Consultar en forma individual los datos de Consumo

5.1.7.1.9.- GESTION DE SALIDA DE CLIENTES (CHECK OUT)

– El sistema deberá permitir:
– Req(34) Ingresar un nuevo Cliente

- Req(35) Eliminar un Cliente
- Req(36) Modificar los datos de un Cliente
- Req(37) Consultar en forma individual los datos de un Cliente

5.1.7.1.10.- GESTION DE GASTOS

- El sistema deberá permitir:
- Req(38) Ingresar un nuevo Gasto
- Req(39) Eliminar un Gasto
- Req(40) Modificar los datos de un Gasto
- Req(41) Consultar en forma individual los datos de un Gasto

5.1.7.1.11.- GESTION TIPOS DE SERVICIOS TELEFONICOS

- El sistema deberá permitir:
- Req(42) Ingresar un nuevo servicio telefónico
- Req(43) Eliminar un servicio telefónico
- Req(44) Modificar los datos de un servicio telefónico
- Req(45) Consultar en forma individual los datos de un servicio telefónico

5.1.7.1.12.- GESTION TIPOS DE GASTOS

- El sistema deberá permitir:
- Req(46) Ingresar un nuevo Tipo de Gasto
- Req(47) Eliminar un Tipo de Gasto
- Req(48) Modificar los datos de un Tipo de Gasto
- Req(49) Consultar en forma individual los datos de un Tipo de Gasto

5.1.7.1.13.- GESTION TIPOS DE CONSUMOS

- El sistema deberá permitir:

- Req(50) Ingresar un nuevo Tipo de Consumo
- Req(51) Eliminar un Tipo de Consumo
- Req(52) Modificar los datos de un Tipo de Consumo
- Req(53) Consultar en forma individual los datos de un Tipo de Consumo

5.1.7.2.- REQUISITOS DE INTERFACES EXTERNAS

En esta sección se describirán los requisitos que afectan a las interfaces externas de usuario e interfaces de comunicación.

5.1.7.2.1.- INTERFACES DE USUARIO

La interfaz debe ser orientada a ventanas y el manejo del programa se realizará a través de teclado y ratón.

5.1.7.2.2.- INTERFACES DE HARDWARE

Los clientes accederán al sistema mediante un modem, el mismo que se conectará a un ISP, Red Privada o también pueden acceder a través de una conexión directa al PBX del ASP.

5.1.7.2.3.- INTERFACES DE SOFTWARE

En la versión inicial el sistema trabajará autónomamente, y no tendrá ninguna interfaz de software con otros sistemas.

5.1.7.2.4.- INTERFACES DE COMUNICACIÓN

La conexión al sistema se la realizará vía Internet o vía un Red Privada, el sistema se encontrará en el Servidor de Aplicaciones y el Servidor Web lo pondrá a disposición en Internet vía una conexión a dos ISP para nivelar el balance de acceso, además se podrá acceder vía conexión directa al PBX del ASP.

5.1.7.3.- REQUISITOS DE DESARROLLO

El ciclo de vida elegido para el desarrollo del sistema es evolutivo de manera que se pueda incorporar fácilmente cambios o agregar mayor funcionalidad al sistema, además en el futuro el sistema se relacionará con otros sistemas para prestar mayores servicios.

5.1.7.4.- REQUISITOS TECNOLOGICOS

Características técnicas del sistema:
Para la correcta operación de la el Sistema Hotelero son necesarios los siguientes elementos de hardware y software:

5.1.7.4.1.- REQUERIMIENTOS DE HARDWARE

5.1.7.4.1.1.- EL SERVIDOR

Un servidor WEB y de base de datos, la configuración de hardware recomendada para el servidor mencionado es la siguiente:

- CD-ROM drive
- 256MB de memoria, 512MB recomendado en Linux
- 100MB de espacio libre en disco para instalación
- Tarjeta de red Ethernet y soporte TCP/IP instalado
- MODEM 65 Kbps

5.1.7.4.1.2.- EL CLIENTE

La configuración de Hardware recomendada para el cliente es el siguiente:

- Pentium I a superior
- 32 MB de Memoria RAM
- 10 MB de Espacio en el Disco Duro
- Tarjeta Ethernet o Tarjeta Fax Modem

5.1.7.4.2.- REQUERIMIENTOS DE SOFTWARE

En esta sección se encuentran los requerimientos de Software bajo los cuales la aplicación va a funcionar.

5.1.7.4.5.2.1.- EL SERVIDOR

Un Servidor WEB que permite presentar los elementos, objetos y componentes del sistema tanto a nivel local como en cada una de las computadoras personales de los Clientes, se recomienda la instalación de Apache Web Server versión 1.3.12 o superior.

Un Motor de base de datos relacional Mysql

5.1.7.4.2.2.- EL CLIENTE

El sistema operativo para los clientes puede ser Windows 9X/Me/NT/2000/XP
Navegadores de Internet: (Microsoft Internet Explorer 4.01, Netscape 4.07 o superiores) en las computadoras personales.

5.1.7.5.- ATRIBUTOS

En los siguientes puntos se tratarán algunos de los requisitos necesarios para un buen desempeño del sistema.

5.1.7.6.- SEGURIDAD

Cuando un usuario intente ingresar al sistema deberá introducir su login y password y el sistema deberá comprobar automáticamente si es un usuario autorizado y que tipo de usuario es, tanto el login y el password no son los correctos entonces el sistema emitirá un mensaje de error

El sistema Hotelero tendrá dos tipos de usuarios y cada uno de ellos se le permitirá únicamente el acceso a aquellas funciones que le correspondan. Los tipos de usuarios que se van a contemplar y las operaciones que cada unos de ellos realiza se describe a continuación.

- Operador: puede Gestionar Centro de Costos, Gestionar habitaciones, Gestionar tipos de servicios telefónicos, tipos de gastos, tipos de consumos, Gestionar las tarifas por temporadas de las Habitaciones, Gestionar reservaciones, Gestionar entradas de clientes, Gestionar consumos, Gestionar llamadas telefónicas, Gestionar salida de clientes, imprimir reportes tales como: reporte de gastos por centro de costos, reporte de consumos por cliente, reporte por tipo de pagos, listado de habitaciones disponibles a la fecha, listado de reservaciones a la fecha.

- Administrador: puede crear usuarios, además de realizar todas la acciones del operador.

5.2.- CONSTRUCCION DEL SISTEMA HOTELERO

La decisión de utilizar UML (Unified Modeling Language – Lenguaje Unificado de Modelado) como notación para nuestro método software se debe a que se ha convertido en un estándar de facto que tiene las siguientes características:

- Permite modelar sistemas utilizando técnicas orientadas a objetos (OO).
- Permite especificar todas las decisiones de análisis, diseño e implementación, construyéndose así modelos precisos, no ambiguos y completos.
- Puede conectarse con lenguajes de programación (Ingeniería directa e inversa).
- Permite documentar todos los artefactos de un proceso de desarrollo (requisitos, arquitectura, pruebas, versiones, entre otros.).
- Cubre las cuestiones relacionadas con el tamaño propio de los sistemas complejos y críticos.

- Es un lenguaje muy expresivo que cubre todas las vistas necesarias para desarrollar y luego desplegar los sistemas.
- Existe un equilibrio entre expresividad y simplicidad, pues no es difícil de aprender ni de utilizar.
- UML es independiente del proceso, aunque para utilizarlo óptimamente se debería usar en un proceso que fuese dirigido por los casos de uso, centrado en la arquitectura, iterativo e incremental.

5.2.1.- ANALISIS DEL SISTEMA

El primer paso para el modelado de una aplicación de negocios es la identificación e los procesos de negocios. En este punto simplemente listamos los procesos que observamos en el documento de especificación de requisitos de software para luego abordarlos uno a uno y asignarlos a cada actor en el diagrama de casos de uso.

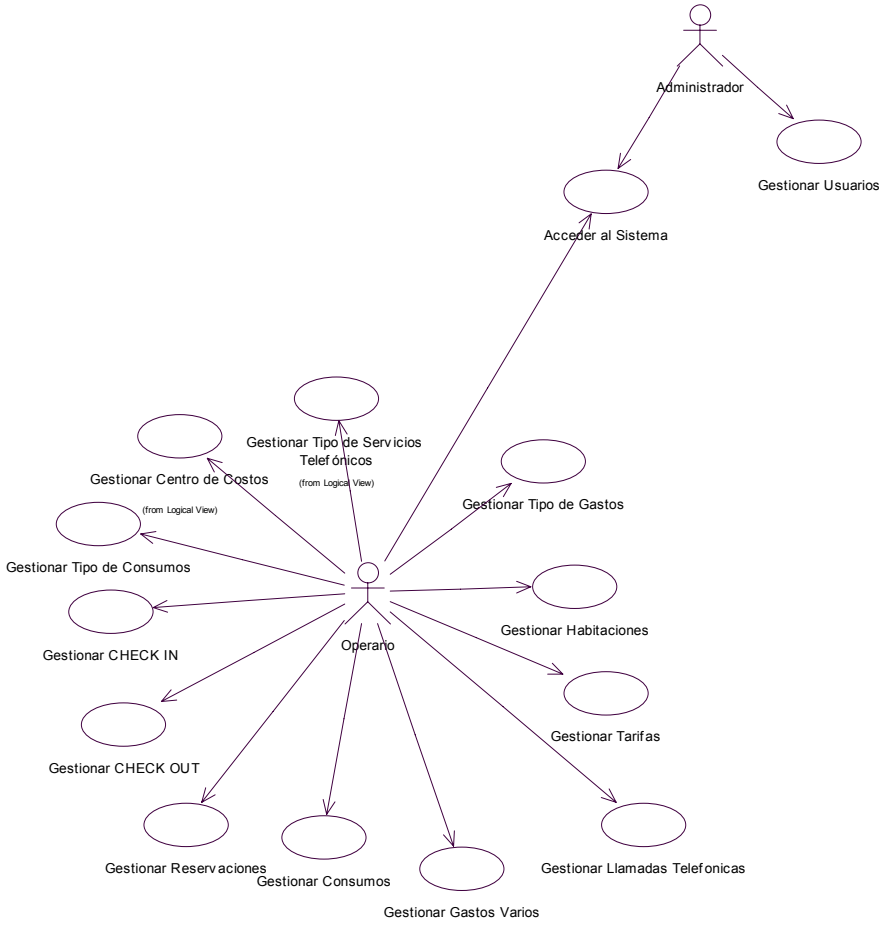
Procesos:

1. Gestión de usuarios
2. Gestión de centro de costos
3. Gestión de gastos
4. Gestión de reservaciones
5. Gestión de registro de entrada de clientes (CHECK IN)
6. Gestión de salida de clientes (CHECK OUT)
7. Gestión de consumos por parte de los clientes en el Hotel
8. Gestión de consumo de llamadas telefónicas por parte de los clientes en el Hotel

5.2.1.1.- Diagrama de Casos de Usos

Luego de conocer los procesos que el sistema debe realizar se procede a diagramar la interacción de los usuarios externos al sistema tales como personas u otros sistemas con los procesos que ellos realizan a esto se le conocen como diagramas de casos de usos

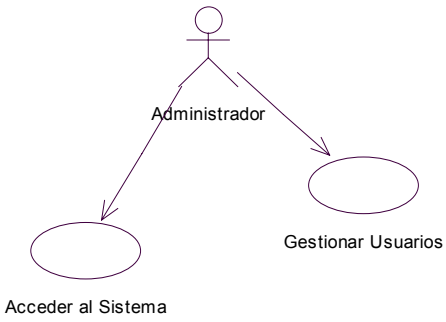
FIGURA V-1 DIAGRAMA DE CASOS DE USO



Descripción de los Casos de Usos

Actor: Administrador:

FIGURA V-2 DIAGRAMA DE CASOS DE USO PARA EL ADMINISTRADOR



1.- Caso de Uso: Crear Usuarios

Objetivo: Crear usuarios en el sistema con sus datos personadles además se debe proporcionar de un login y password que les servirá para ingresar al sistema

Actores: Administrador

Precondiciones:

Pasos:

1(A): Indicar que usuario se va a registrar

2(S): Verificar que el usuario no este registrado

3(S): Verificar que su login no este utilizado por otro usuario

4(A): Registrar el Usuario

Variaciones:

2. a.- Si existe el usuario registrado

2. a.1.- Emitir mensaje de error

2. a.2.- Finalizar caso de uso
3. a.- Si otro usuario ya tiene el mismo login
3. a.1.- Emitir mensaje de error
3. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

2.- Caso de Uso: Acceder al Sistema

Objetivo: Permitir al Administrador o Operarios del sistema ingresar al sistema, previo la verificación de un login y password

Actores: Administrador, Operarios

Precondiciones:

Pasos:
1(A): Indicar que usuario se va a ingresar al sistema
2(S): Verificar que el login y password son correctos
3(A): Ingresar al Sistema

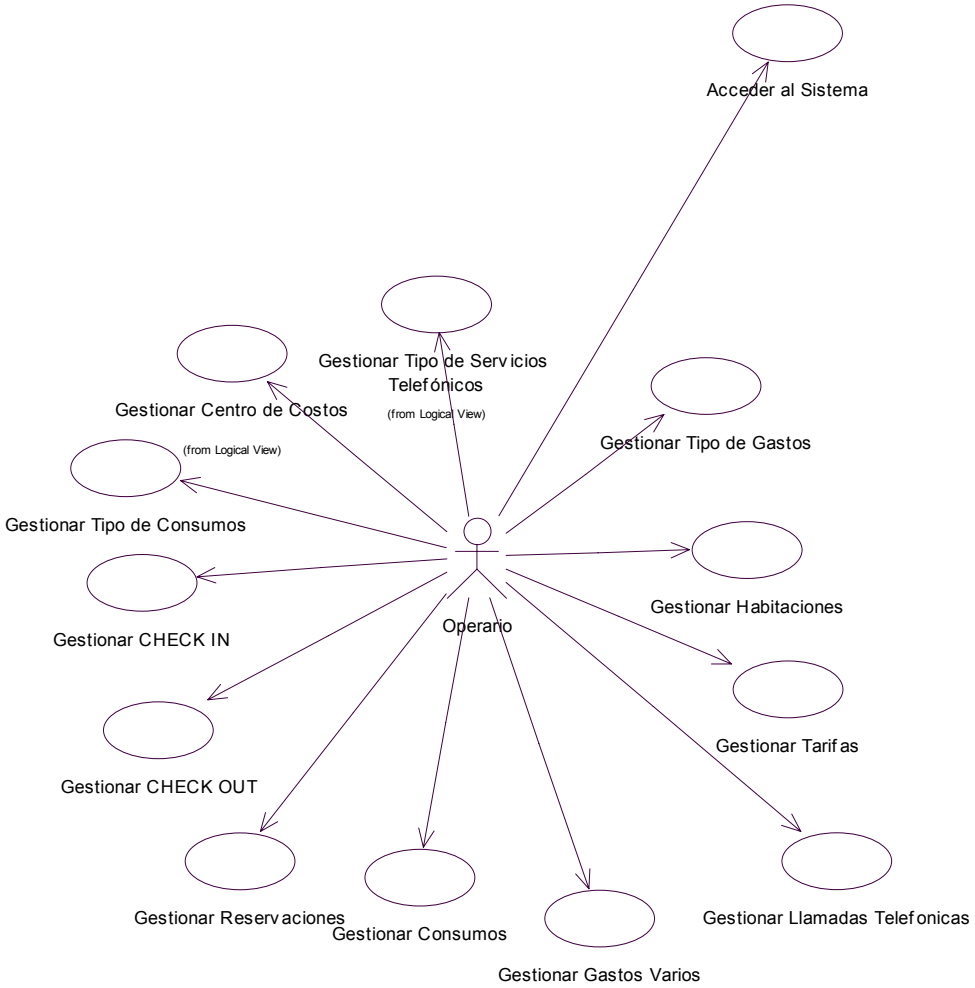
Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

Actor: Operario

FIGURA V-3 DIAGRAMA DE CASOS DE USO PARA EL OPERARIO



3.- Caso de Uso: Acceder al Sistema

Objetivo: Permitir al Administrador o Operarios del sistema ingresar al sistema, previo la verificación de un login y password

Actores: Administrador, Operarios

Precondiciones:

Pasos:
1(A): Indicar que usuario se va a ingresar al sistema
2(S): Verificar que el login y password son correctos
3(A): Ingresar al Sistema

Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

4.- Caso de Uso: Gestionar Tipos de Gastos

Objetivo: Gestionar los diferentes gastos en los cuales el Hotel incurre

Actores: Operarios

Precondiciones:

Pasos:

1(A): Indicar el tipo de gasto ha ser registrado
2(S): Verificar que los datos son correctos y requeridos
3(A): Gestionar Tipo de Gasto

Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:
Cuestiones:

5.- Caso de Uso: Gestionar Habitaciones

Objetivo: Gestionar las Habitaciones con las cuales el Hotel cuenta y van a ser puestas a disposición de los clientes

Actores: Operarios

Precondiciones: Que exista el Centro de Costos Habitaciones

Pasos:
1(A): Ingresar datos de la Habitación
2(S): Verificar que los datos son correctos y requeridos
3(A): Gestionar Habitación

Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

6.- Caso de Uso: Gestionar Tarifas

Objetivo: Gestionar las tarifas de las Habitaciones por temporadas (Alta, Media, Baja)

Actores: Operarios

Precondiciones:

Pasos:

1(A): Ingresar las tarifas de la Habitación con las fechas de inicio y fin de temporada y el porcentaje de incremento en el valor de Habitación

2(S): Verificar que los datos son correctos y requeridos

3(A): Gestionar Tipo de Gasto

Variaciones:

2. a.- Si no son correctos

2. a.1.- Emitir mensaje de error

2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

7.- Caso de Uso: Gestionar Llamadas telefónicas

Objetivo: Gestionar las llamadas telefónicas que los clientes realizan

Actores: Operarios

Precondiciones:

-EL cliente debe estar registrado en la tarjeta de registro y su reservación debe estar activa

Pasos:

1(A): Ingresar datos del Cliente que realiza la llamada telefónica

2(S): Verificar que el cliente existe en la tarjeta de registro y su reservación esta activa

3(A): Gestionar al cliente el la llamada telefónica realizada por el valor de la llamada

Variaciones:

2. a.- Si el cliente no esta registrado en la tarjeta de registro

2. a.1.- Emitir mensaje de error

2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

8.- Caso de Uso: Gestionar Consumos

Objetivo: Gestionar consumos de los clientes hospedados en el Hotel

Actores: Operarios

Precondiciones:

-EL cliente debe estar registrado en la tarjeta de registro y su reservación debe estar activa

Pasos:

1(A): Ingresar datos del Cliente que realiza el Consumo

2(S): Verificar que el cliente existe en la tarjeta de registro y su reservación esta activa

3(A): Gestionar al cliente el consumo realizado y el valor por el consumo

Variaciones:

2. a.- Si el cliente no esta registrado en la tarjeta de registro

2. a.1.- Emitir mensaje de error

2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

9.- Caso de Uso: Gestionar Reservaciones

Objetivo: Gestionar las reservaciones que soliciten los clientes en esta reservación esta estrictamente relacionada con la disponibilidad de Habitaciones que en ese momento el Hotel tenga

Actores: Operarios

Precondiciones:
-Que exista el Centro de Costos Reservaciones
-Que existan Habitaciones disponibles

Pasos:
1(A): Ingresar datos de la Reservación
2(S): Verificar que los datos son correctos y requeridos
3(A): Gestionar Reservación

Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

10.- Caso de Uso: Gestionar CHECK IN

Objetivo: Gestionar el ingreso de los clientes en la tarjeta de registro del Hotel con datos esenciales que el hotel como el ministerio de turismo requiere

Actores: Operarios

Precondiciones:
-Que exista una previa Reservación y esta este activa

Pasos:
1(A): Ingresar datos del Cliente
2(S): Verificar que los datos son correctos y requeridos

3(A): Gestionar Ingreso de Clientes en Tarjeta de Registro

Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

11.- Caso de Uso: Gestionar CHECK OUT

Objetivo: Gestionar la salida de los clientes del Hotel con datos esenciales que el hotel como el ministerio de turismo requiere

Actores: Operarios

Precondiciones:
-Que el cliente este previamente registrado en la tarjeta de registro de ingreso

Pasos:
1(S): Verificar que el cliente este registrado en la tarjeta de registro
2(A): Gestionar datos de salida del Cliente

Variaciones:
1. a.- Si no existen datos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

12.- Caso de Uso: Gestionar Tipos de Consumos

Objetivo: Gestionar los diferentes gastos en los cuales el Hotel incurre

Actores: Operarios

Precondiciones:

Pasos:
1(A): Ingresar el tipo de consumo
2(S): Verificar que los datos son correctos y requeridos
3(A): Gestionar Tipo de Consumo

Variaciones:
2. a.- Si no son correctos
2. a.1.- Emitir mensaje de error
2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

13.- Caso de Uso: Gestionar Tipos de Servicios Telefónicos

Objetivo: Gestionar los diferentes tipos de servicios telefónicos a disposición de los clientes del hotel

Actores: Operarios

Precondiciones:
Que exista el centro de costos para asociarlo al tipo de servicio telefónico

Pasos:

1(A): Ingresar el tipo de servicio telefónico

2(S): Verificar que los datos son correctos y requeridos

3(A): Gestionar Tipo de servicio

Variaciones:

2. a.- Si no son correctos

2. a.1.- Emitir mensaje de error

2. a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

14.- Caso de Uso Gestionar Centro de Costos

Actores: Operario (iniciador)

Propósito: Registra los centro de costos que el hotel utiliza para tener organizado y se podrá conocer todos los gastos de ingreso o egreso que los centros de costos generan

Visión General:

Tipo: Primario y esencial

Referencia: Requisito 3.1.2

Curso: Típico de Eventos

1.- (O)El operario selecciona el menú centro de costos

2.- (S)El Sistema despliega el formulario de centro de costos

3- (S) El sistema presenta un listado de los centros de costos existentes

4.- (O) El operario ingresa el nuevo centro costos

5.- (O) Se registra el nuevo centro de costos

Cursos Alternativos:

15.- Caso de Uso: Gestionar Tipos de Consumos

Objetivo: Gestionar los diferentes tipos de consumos

Actores: Operarios

Precondiciones:
Que exista en Centro de Costo del Consumo

Pasos:
1(A): Ingresar el tipo de consumo
2(S): Verificar que los datos son correctos y requeridos
3(A): Gestionar Tipo de Consumo

Variaciones:
2.a.- Si no son correctos
2.a.1.- Emitir mensaje de error
2.a.2.- Finalizar caso de uso

Extensiones:

Cuestiones:

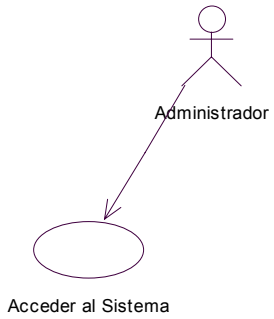
5.2.1.2.- Diagrama de Casos de Uso Expandido

Este diagrama va dirigido al equipo desarrollador del proyecto ya es un poco más técnico y más descriptivo de los procesos que el sistema debe realizar

1.- Caso de Uso Acceder al Sistema

1.- Actores: Administrador (iniciador)

FIGURA V-4. DIAGRAMA DE CASOS DE USO ADMINISTRADOR ACCEDE AL SISTEMA



Propósito: Permite Ingresar al sistema mediante un login y password para poder realizar sus operaciones

Visión General:

Tipo: Primario y esencial

Referencia: Requisito

Curso: Típico de Eventos

1.-(S)El sistema presenta un formulario de ingreso de datos de usuario

2.- (A)El administrador ingreso login y password

3.- (A)Presiona sobre aceptar

4.- (S)El Sistema verifica si el usuario esta registrado como tal

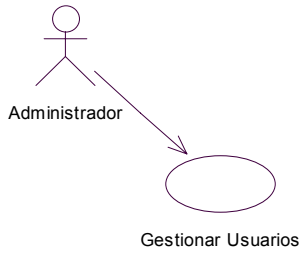
3- (A) El Administrador ingresa al sistema

Cursos Alternativos:

4.1(S)Si el usuario no existe el sistema emite mensaje de error

2.- Caso de Uso Gestionar Usuarios

FIGURA V-5. DIAGRAMA DE CASOS DE USO ADMINISTRADOR GESTIONAR USUARIOS



Actores: Administrador (iniciador)

Propósito: Registra los usuarios que tendrán el perfil de operarios del sistema básicamente ellos son los que operaran el sistema Hotelero

Visión General:

Tipo: Primario y esencial

Referencia: Req(1), Req(2), Req(3), Req(4): (Gestionar Usuario)

Curso: Típico de Eventos

1.- (A)El administrador selecciona el menú usuarios

2.- (S)El Sistema despliega el formulario de usuarios

3- (A) El sistema presenta un listado de los usuarios registrados

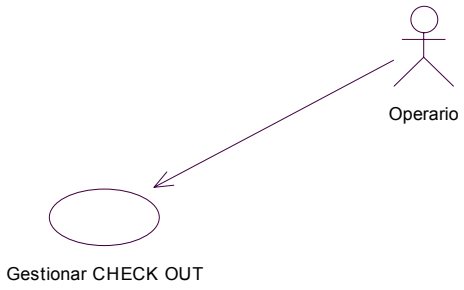
4.- (A) El operario ingresa un nuevo usuario

5.- (A) Registra el nuevo centro de costos

Cursos Alternativos:

3.- Caso de Uso Gestionar CHECK OUT

FIGURA V-6. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR CHECK OUT



Actores: Operador (iniciador)

Propósito: Registra en la tarjeta de registro de salida del cliente al Hotel

Visión General:

Tipo: Primario y esencial

Referencia: Req(34), Req(35), Req(36), Req(37): Gestionar CHECK OUT

Curso: Típico de Eventos

1.- (O)El operario selecciona el menú CHECK OUT

2.-(S) El sistema despliega el listado de los clientes registrados

3.-(O)Selecciona el Cliente al cual se le va ha realizar CHECK OUT

4.- (O) El operario ingresa datos del cliente

5.- (O) Se registra el CHECK OUT

Cursos Alternativos:

4.- Caso de Uso Gestionar CHECK IN

FIGURA V-7. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR CHECK IN

Actores: Operador (iniciador)

Propósito: Registra en la tarjeta de registro el ingreso del cliente al Hotel

Visión General:

Tipo: Primario y esencial

Referencia: Req(22), Req(23), Req(24), Req(25): Gestionar CHECK IN

Curso: Típico de Eventos

1.- (O)El operario selecciona el menú CHECK IN

2.- (S)El Sistema despliega el formulario tarjeta de registro

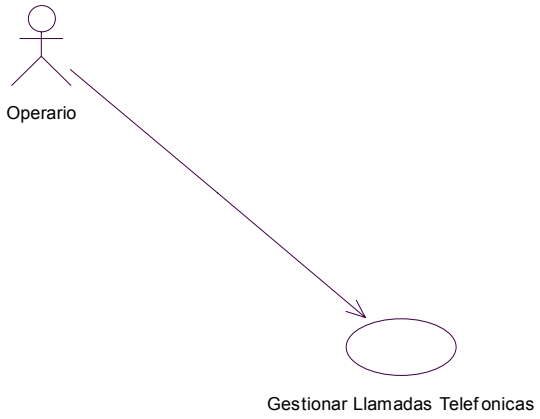
4.- (O) El operario gestiona el CHECK IN

5.- (O) Se registra la operación

Cursos Alternativos:

5.- Caso de Uso Gestionar Llamadas telefónicas

FIGURA V-8. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR LLAMADAS TELEFÓNICAS



Actores: Operador (iniciador)

Propósito: Registra las llamadas telefónicas que los clientes realizan

Visión General:

Tipo: Primario y esencial

Referencia: Req(26), Req(27), Req(28), Req(29): Gestionar consumo llamadas telefónicas

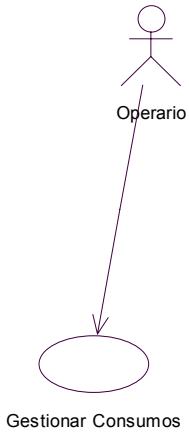
Curso: Típico de Eventos

1.- (O) El operario selecciona el menú Consumos
2.-(S) El sistema despliega el listado de los clientes registrados
3.-(O) Selecciona el Cliente al cual se le va ha gestionar la llamada
4.- (O) El operario ingresa datos del consumo de la llamada telefónica
5.- (O) Se registra el consumo

Cursos Alternativos:

6.- Caso de Uso Gestionar Consumos

FIGURA V-9. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR CONSUMOS



Actores: Operador (iniciador)

Propósito: Registra los consumos que los clientes realizan

Visión General:

Tipo: Primario y esencial

Referencia: Req(30), Req(31), Req(32), Req(33): Gestionar consumos

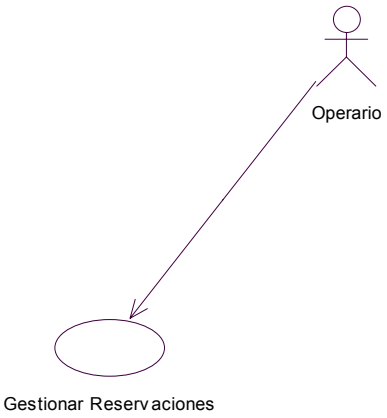
Curso: Típico de Eventos

1.- (O)El operario selecciona el menú Consumos
2.-(S) El sistema despliega el listado de los clientes registrados
3.-(O)Selecciona el Cliente al cual se le va ha gestionar el Consumo
4.- (O) El operario ingresa datos del consumo
5.- (O) Se registra el consumo

Cursos Alternativos:

7.- Caso de Uso Gestionar Reservaciones

FIGURA V-10. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR RESERVACIONES



Actores: Operador (iniciador)

Propósito: Registra las reservaciones de los clientes en el sistema
Visión General:

Tipo: Primario y esencial

Referencia: Req(18), Req(19), Req(20), Req(21): Gestionar Reservaciones

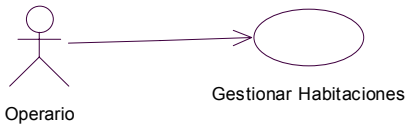
Curso: Típico de Eventos

1.- (O)El operario selecciona el menú reservaciones
2.- (S)El Sistema despliega el formulario de reservaciones
3- (S) El sistema presenta un listado de las reservaciones del hotel
4.- (O) El operario gestiona la reservación
5.- (O) Se registra la operación

Cursos Alternativos:

8.- Caso de Uso Gestionar Habitaciones

FIGURA V-11. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR HABITACIONES



Actores: Operario (iniciador)

Propósito: Registra las habitaciones que podrán ser reservadas por los clientes

Visión General:

Tipo: Primario y esencial

Referencia: Req(10), Req(11), Req(12), Req(13): Gestionar Habitaciones

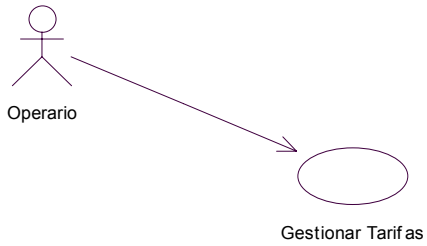
Curso: Típico de Eventos

1.- (O)El operario selecciona el menú habitaciones
2.- (S)El Sistema despliega el formulario de registro de habitaciones
3- (S) El sistema presenta un listado de las habitaciones
4.- (O) El operario ingresa un nuevo centro de costos con la operación a realizar
5.- (O) Se registra el nuevo centro de costos

Cursos Alternativos:

9.- Caso de Uso Gestionar Tarifas

FIGURA V-12. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR TARIFAS



Actores: Operario(iniciador)

Propósito: Registra las tarifas que utilizaran el hotel, existen tres tipos de temporadas en los cuales se aplican tres tipos de tarifas diferentes

Visión General:

Tipo: Primario y esencial

Referencia: caso de uso Gestionar Habitaciones

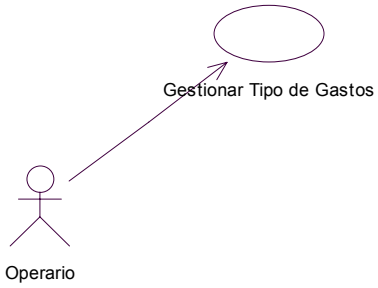
Curso: Típico de Eventos

1.- (O)El operario selecciona el menú tarifas
2.- (S)El Sistema despliega el formulario de para la gestión de tarifas
4.- (O) El operario gestionar tarifa
5.- (O) Se registra las nuevas tarifas

Cursos Alternativos:

10.- Caso de Uso Gestionar Tipos de Gastos

FIGURA V-13. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR TIPO DE GASTOS



Actores: Operario (iniciador)

Propósito: Registra los tipos de gastos que incurre el hotel

Visión General:

Tipo: Primario y esencial

Referencia: caso de uso gestionar gastos

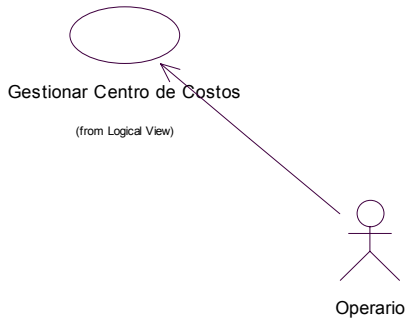
Curso: Típico de Eventos

1.- (O)El operario selecciona el menú tipo de gastos
2.- (S)El Sistema despliega el formulario tipos de gastos
3- (S) El sistema presenta un listado de los tipos de gastos existentes
4.- (O) El operario ingresa el nuevo tipo de gasto
5.- (O) Se registra el nuevo tipo de gasto

Cursos Alternativos:

11.- Caso de Uso Gestionar Centro de Costos

FIGURA V-14. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR CENTRO DE COSTOS



Actores: Operario (iniciador)

Propósito: Registra los centro de costos que el hotel utiliza para tener organizado y se podrá conocer todos los gastos de ingreso o egreso que los centros de costos generan

Visión General:

Tipo: Primario y esencial

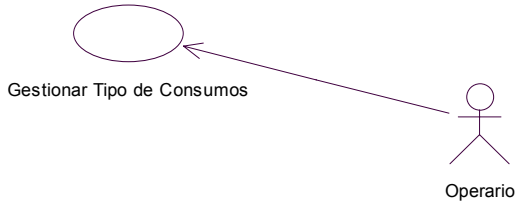
Referencia: Req(06), Req(07), Req(08), Req(09): Gestionar Centro de Costos
Curso: Típico de Eventos

1.- (O)El operario selecciona el menú centro de costos
2.- (S)El Sistema despliega el formulario de centro de costos
3- (S) El sistema presenta un listado de los centros de costos existentes
4.- (O) El operario ingresa el nuevo centro costos
5.- (O) Se registra el nuevo centro de costos

Cursos Alternativos:

12.- Caso de Uso Gestionar Tipos de Consumos

FIGURA V-15. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR TIPOS DE CONSUMO



Actores: Operario (iniciador)

Propósito: Registra los tipos de consumos comunes que el usuarios realiza

Visión General:

Tipo: Primario y esencial

Referencia: caso de uso Consumos

Curso: Típico de Eventos

1.- (O)El operario selecciona el menú tipo de consumos
2.- (S)El Sistema despliega el formulario tipos de consumos
3- (S) El sistema presenta un listado de los tipos de consumos existentes
4.- (O) El operario ingresa el nuevo tipo de consumo
5.- (O) Se registra el nuevo tipo de consumo

Cursos Alternativos:

13.- Caso de Uso Gestionar Tipos de Servicios Telefónicos

FIGURA V-16. DIAGRAMA DE CASOS DE USO OPERARIO GESTIONAR TIPOS DE SERVICIOS TELEFÓNICOS

Actores: Operario (iniciador)

Propósito: Registra los tipos de servicios telefónicos que se encuentran a disposición de los cliente del Hotel

Visión General:

Tipo: Primario y esencial

Referencia: Caso de uso gastos

Curso: Típico de Eventos

1.- (O)El operario selecciona el menú tipo de
Servicios telefónicos

2.- (S)El Sistema despliega el formulario tipos de
Servicios telefónicos

3- (S) El sistema presenta un listado de los tipos de servicios telefónicos existentes

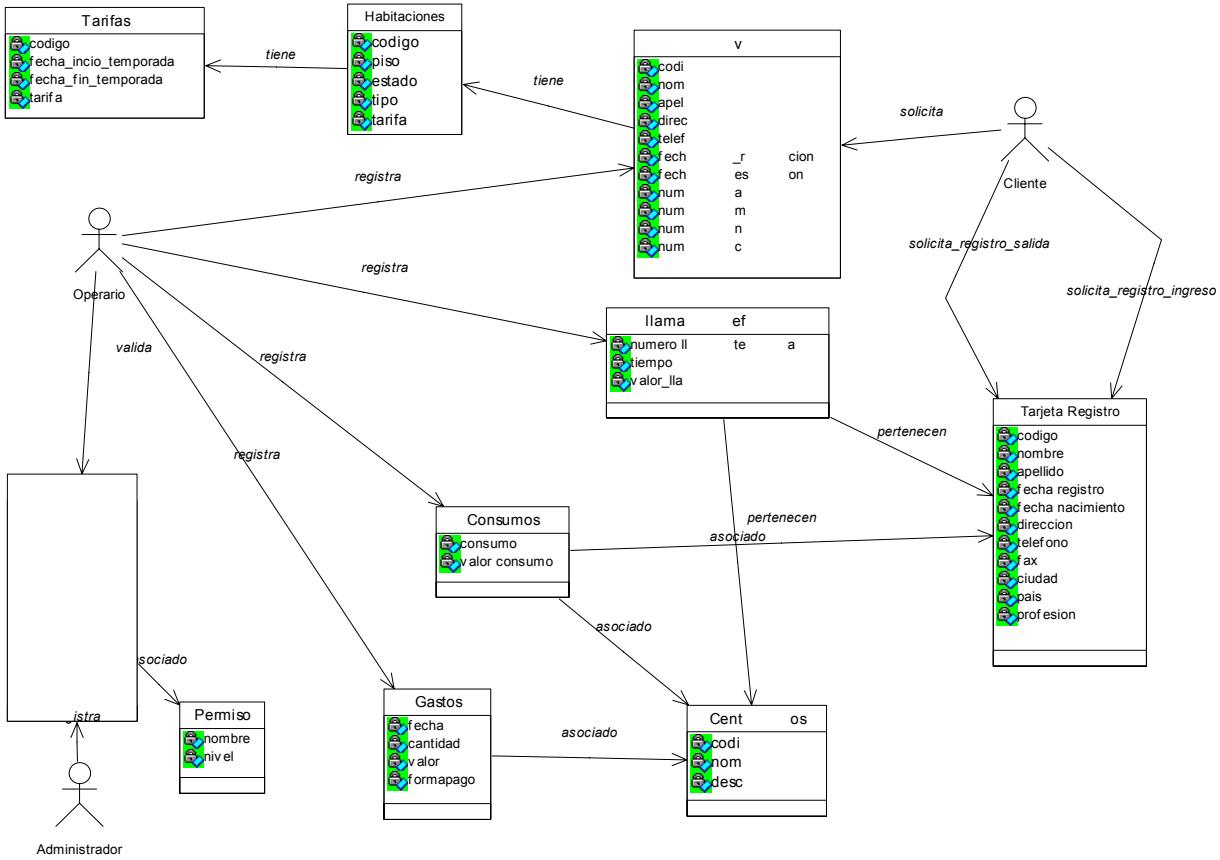
4.- (O) El operario ingresa el nuevo tipo de servicio telefónico

5.- (O) Se registra el nuevo tipo de servicios telefónico

Cursos Alternativos:

5.2.1.3.- Diagrama Conceptual

FIGURA V-17 DIAGRAMA DE CONCEPTUAL DEL SISTEMA HOTELERO



5.2.2.- Diseño del Sistema

Para el diseño del sistema se utilizó los diagramas de secuencia que muestran la interacción ordenada según la secuencia temporal de eventos. En particular, muestra los objetos participantes en la interacción y los mensajes que intercambian ordenados según su secuencia en el tiempo, además los diagramas de colaboración muestra una interacción organizada basándose en los objetos que toman parte en la interacción y en los enlaces entre los mismos

1.- Gestionar Centro de Costos

Diagrama de Secuencia

FIGURA V-18 DIAGRAMA DE SECUENCIA GESTIONAR CENTRO

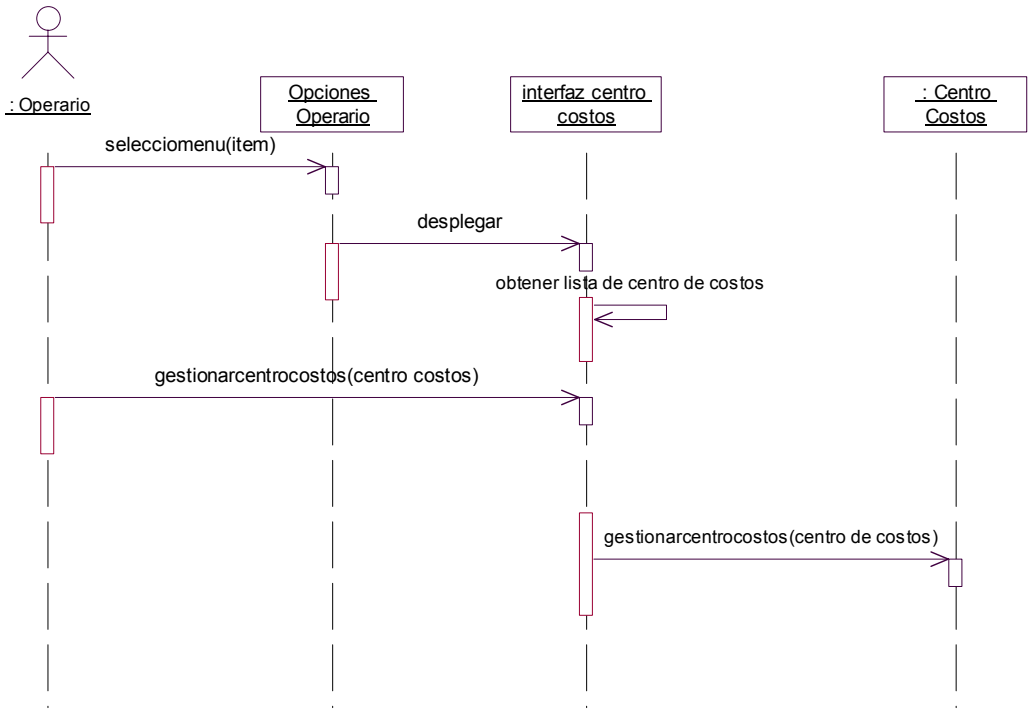
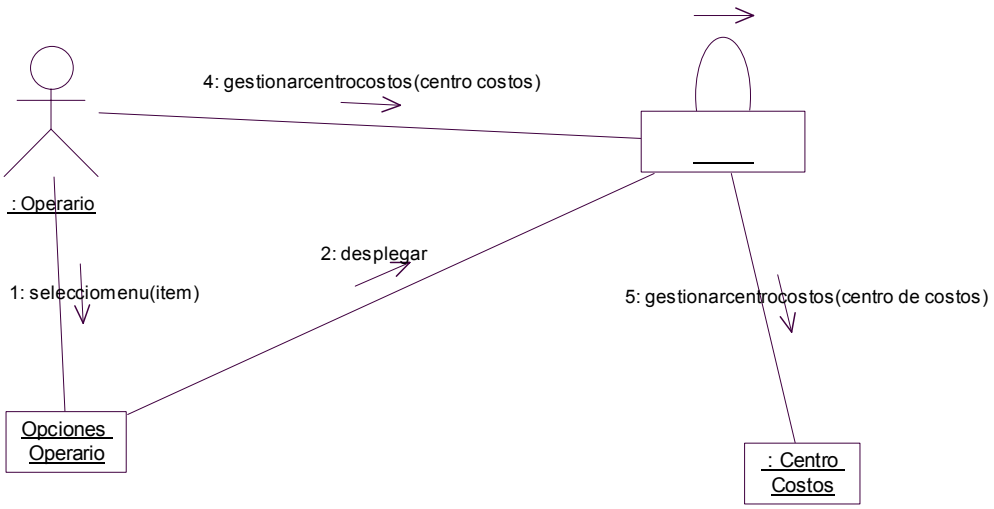


Diagrama de Colaboración

FIGURA V-19 DIAGRAMA DE COLABORACIÓN GESTIONAR CENTRO



Contrato de Operación

Nombre: gestionarcentrocosto(centrocosto):boolean

Responsabilidad: Permite Gestionar un nuevo centro de costos del hotel, para cada centro de costo se requiere la siguiente información (código, nombre, descripción), el sistema debe calcular los ingresos y egresos en función a centro de costos

Tipo: Centro Costos

Caso de Uso: Gestionar Centro de Costo

Notas:

Excepciones:

Salidas:

Precondiciones:

Postcondiciones: Un objeto centro costos es creado

2.- Gestionar Tarifas

Diagrama de Secuencia

FIGURA V-20 DIAGRAMA DE SECUENCIA GESTIONAR TARIFAS

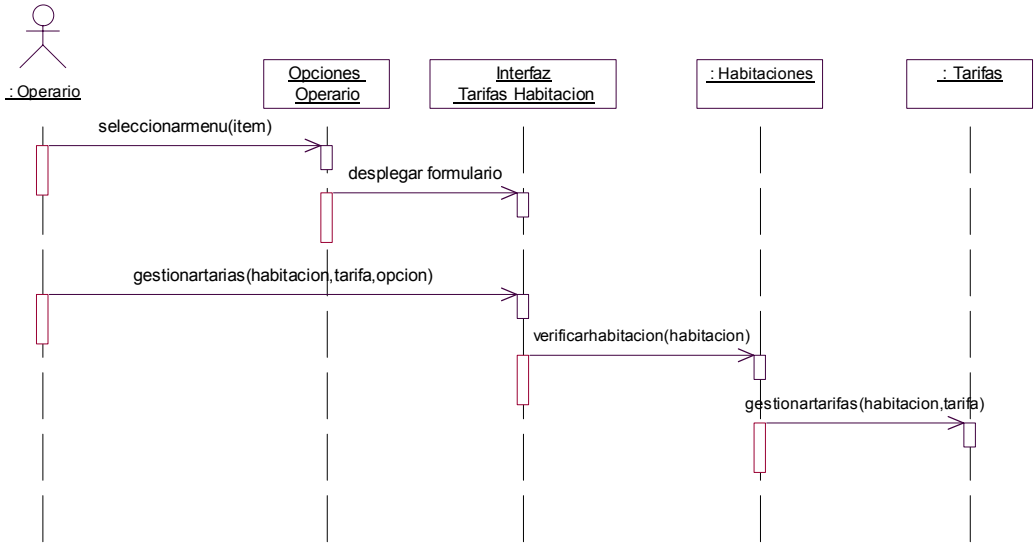
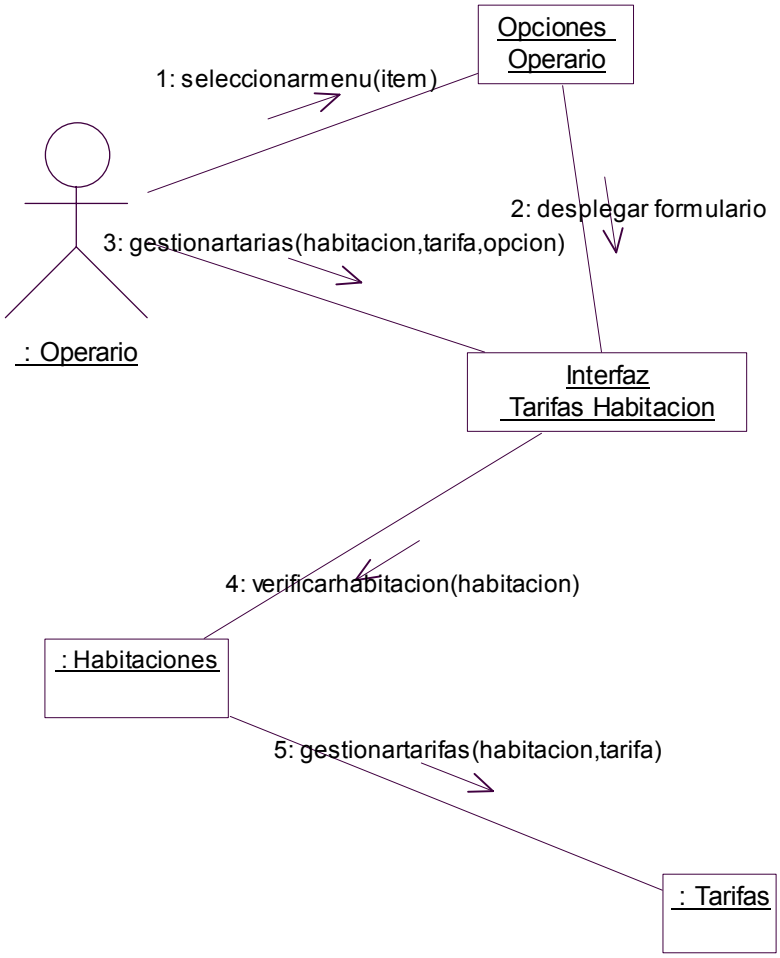


Diagrama de Colaboración

FIGURA V-22 DIAGRAMA DE COLABORACIÓN GESTIONAR TARIFAS



Contrato de Operación

Nombre: gestionartarifas(tarifa,habitacion):boolean

Responsabilidad: Permite gestionar las tarifas, el sistema debe tener en cuenta las tarifas para realizar el incremento o decremento del un porcentaje en el precio de la habitación automáticamente dependiendo de la temporada en la que se encuentre existen tres tipo de temporadas alta, media y baja

Tipo: Tarifa

Caso de Uso: Gestionar Tarifas

Notas:

Excepciones:

Salidas:

Precondiciones:

Postcondiciones: Un objeto tarifa es creado

3.- Gestionar Habitaciones

Diagrama de Secuencia

FIGURA V-23 DIAGRAMA DE SECUENCIA GESTIONAR HABITACIONES

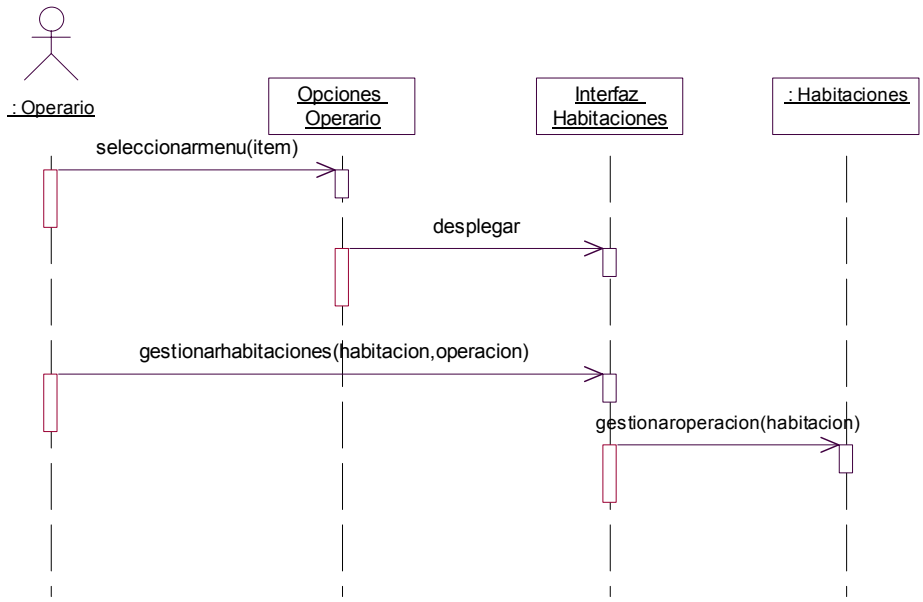
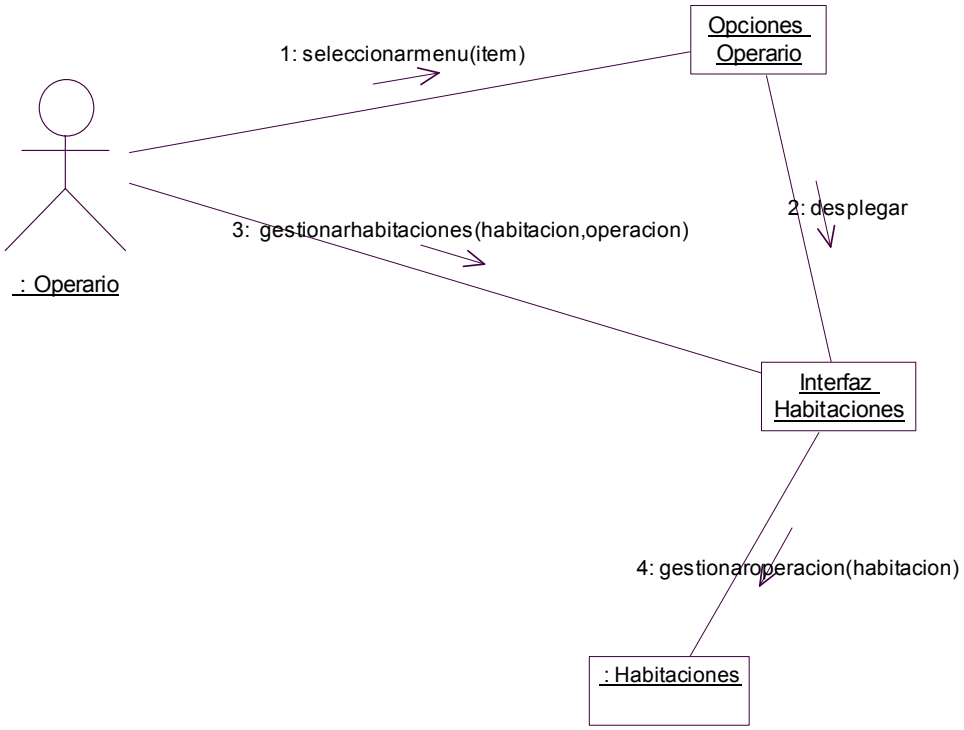


Diagrama de Colaboración

FIGURA V-24 DIAGRAMA DE COLABORACIÓN GESTIONAR HABITACIONES



Contrato de Operación

Nombre: gestionarhabitaciones(habitaciones,operacion):boolean

Responsabilidad: Permite gestionar las habitaciones que el hotel pondrá a disposición a los clientes las habitaciones pertenecen al centro de costos Habitaciones

Tipo: Habitaciones

Caso de Uso: Gestionar Habitaciones

Notas:

Excepciones:

Salidas:

Precondiciones: Tener registrado el centro de costos de habitaciones y las tarifa correspondiente

Postcondiciones: Un objeto habitaciones es creado

4.- Gestionar Reservaciones

Diagrama de Secuencia

FIGURA V-25 DIAGRAMA DE SECUENCIA GESTIONAR RESERVACIONES

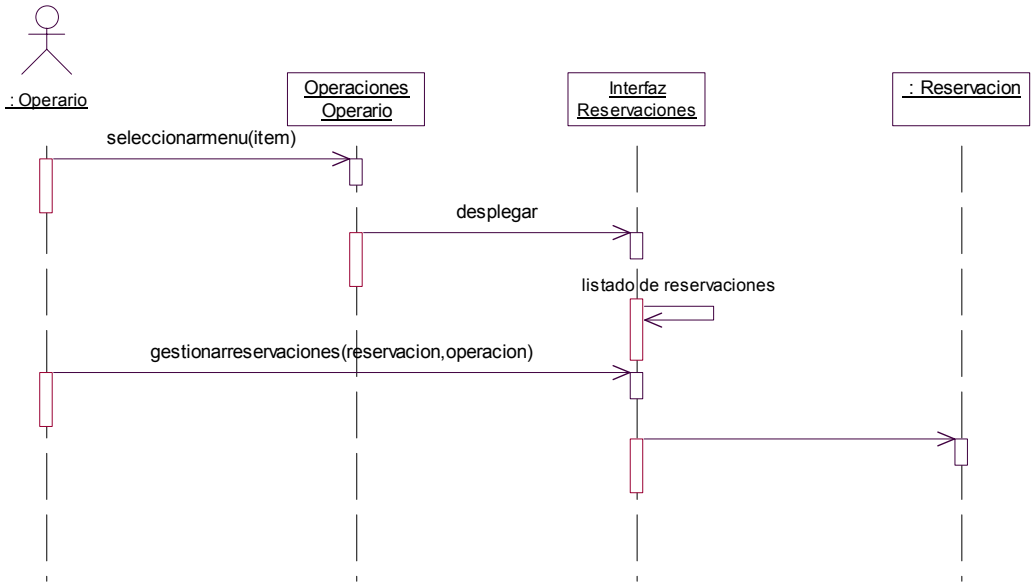
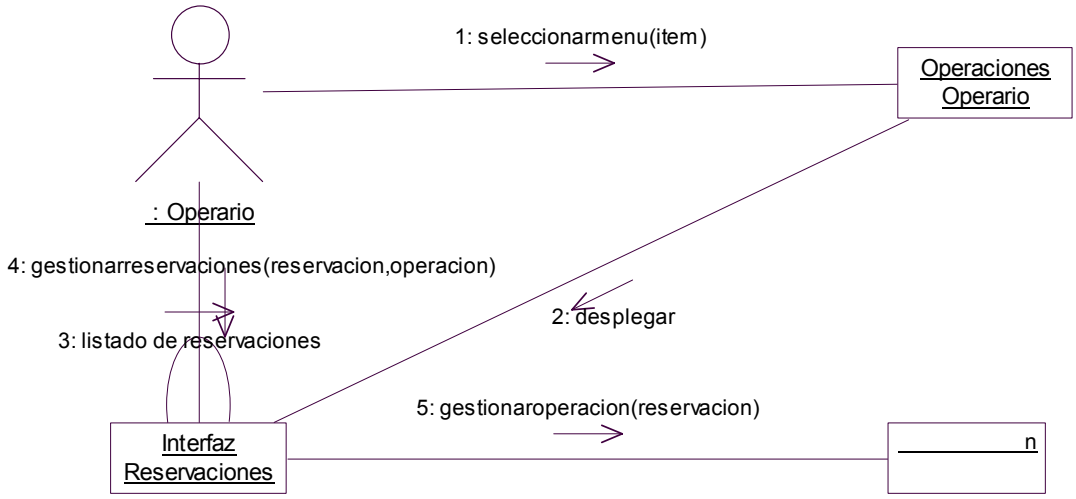


Diagrama de Colaboración

FIGURA V-26. DIAGRAMA DE COLABORACIÓN GESTIONAR RESERVACIONES



Contrato de Operación

Nombre: gestionar reservaciones(reservacion,operacion):boolean

Responsabilidad: Permite gestionar las operaciones que se realizara sobre las reservaciones de los clientes, en la reservación el sistema automáticamente mostrará las habitaciones disponibles en las fechas de inicio de la reservación y finalización de la reservación.

Tipo: Reservación

Caso de Uso: Gestionar Reservación

Notas:

Excepciones:

Salidas:

Precondiciones: Que se encuentre registrado previamente el centro de costos reservación

Postcondiciones: Un objeto reservación se ha creado

5.- Gestionar CHECK IN

Diagrama de Secuencia

FIGURA V-27 DIAGRAMA DE SECUENCIA GESTIONAR CHECK IN

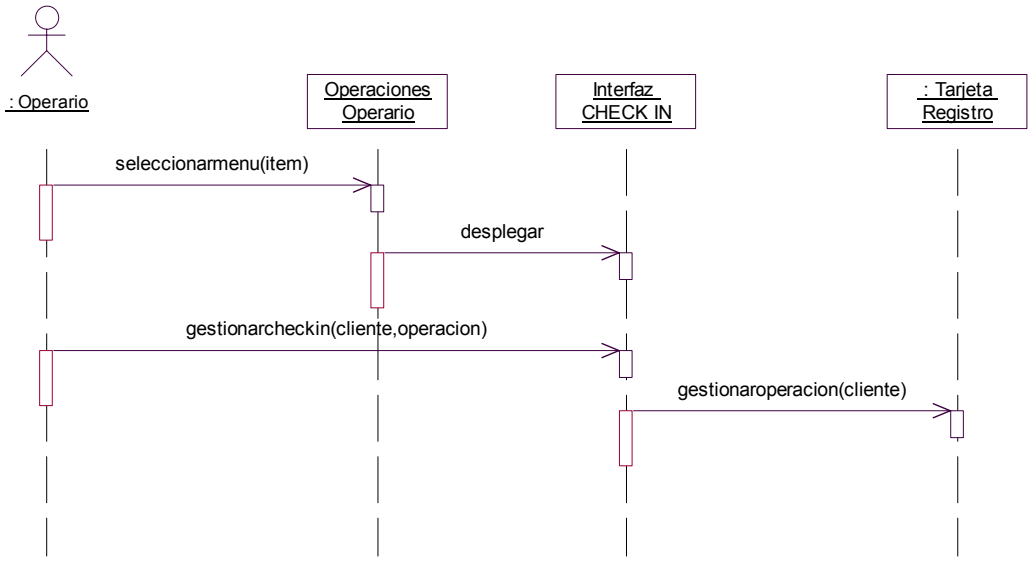
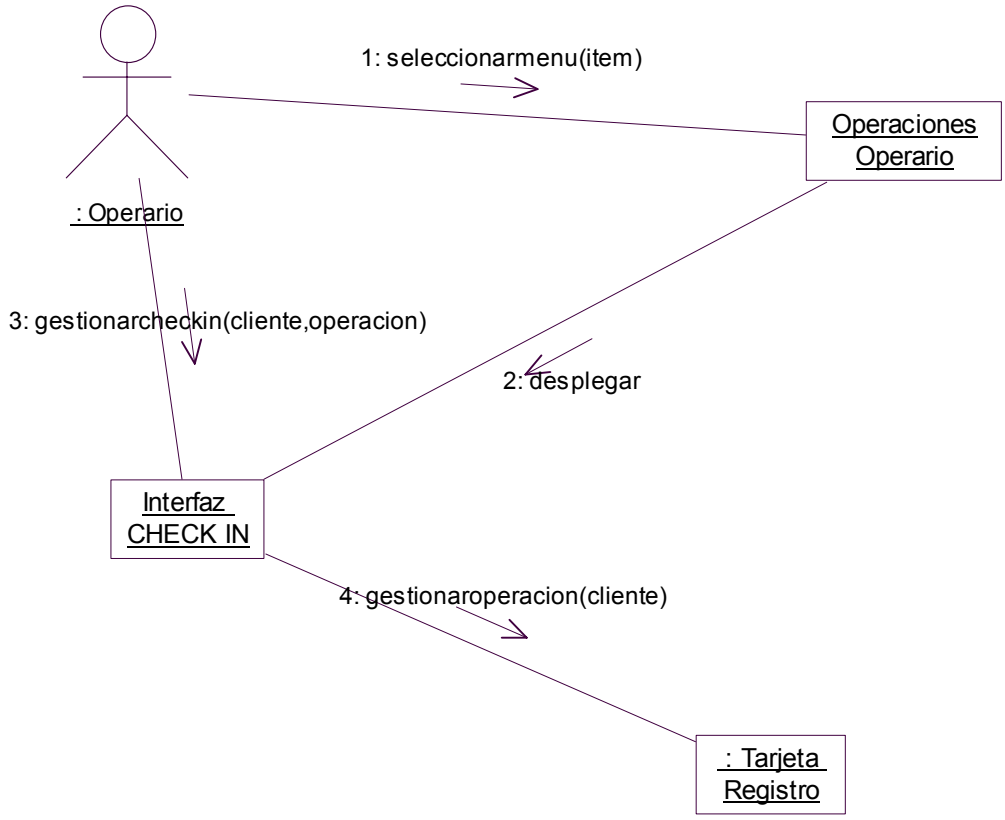


Diagrama de Colaboración

FIGURA V-28 DIAGRAMA DE COLABORACIÓN GESTIONAR CHECK IN



Contrato de Operación

Nombre: gestionarcheckin(datosingresotarjetaregistro,operacion):boolean

Responsabilidad: Permite gestionar las operaciones que se realizara sobre el registro de ingreso al hotel de los cliente, ya que solamente los clientes que se encuentren registrados en la tarjeta de registro podrán realizar consumos o llamadas telefónicas

Tipo: Reservación

Caso de Uso: Gestionar CHECK IN

Notas:

Excepciones:

Salidas:

Precondiciones: Que se el cliente haya tenido una previa reservación

Postcondiciones: Un nuevo cliente se ha registrado en la tarjeta registro

6.- Gestionar CHECK OUT

Diagrama de Secuencia

FIGURA V-29 DIAGRAMA DE SECUENCIA GESTIONAR CHECK OUT

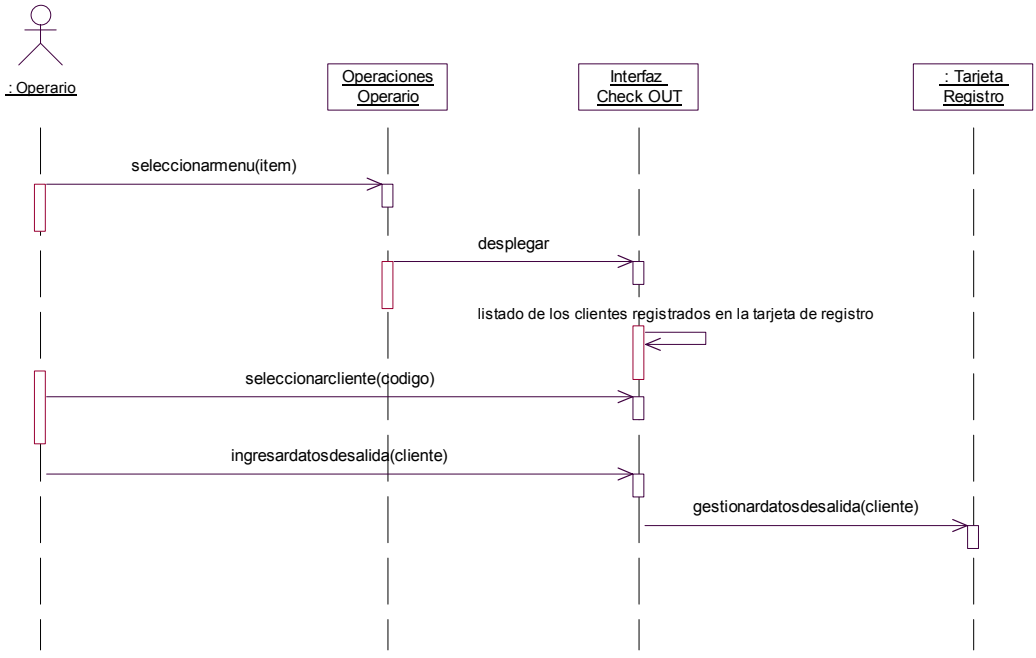
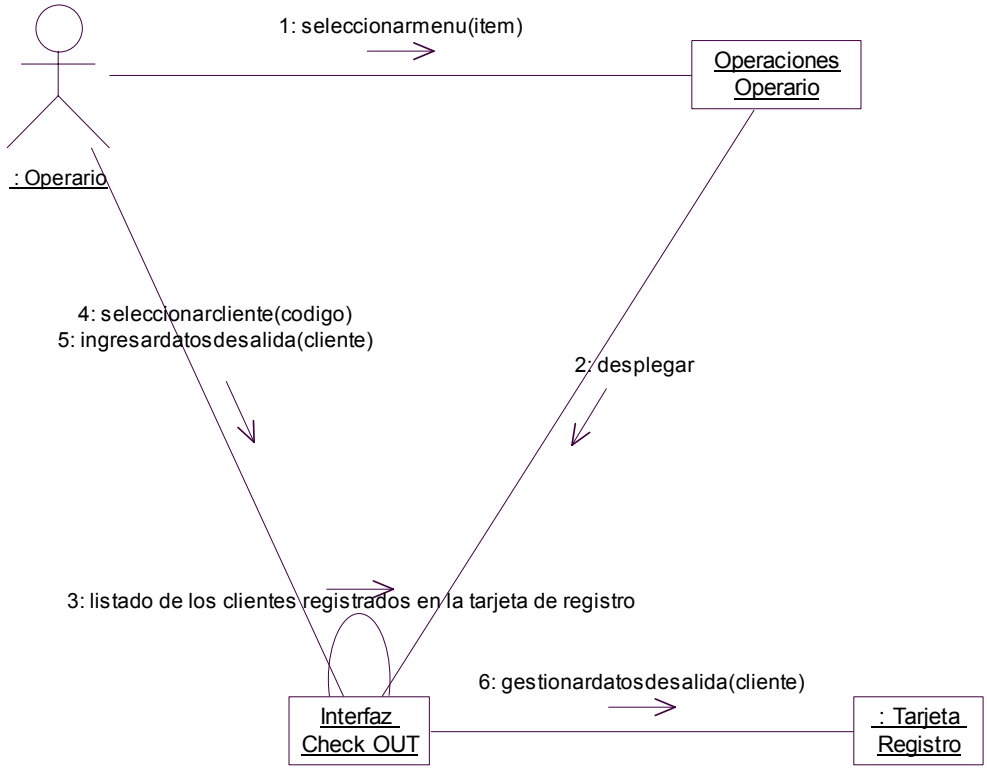


Diagrama de Colaboración

FIGURA V-30. DIAGRAMA DE COLABORACIÓN GESTIONAR CHECK OUT



Contrato de Operación

Nombre: gestionarcheckout(datosingresotarjetaregistro,operacion):boolean

Responsabilidad: Permite Gestionar en la tarjeta de registro la salida del cliente del hotel

Tipo: Reservación

Caso de Uso: Gestionar CHECK OUT

Notas:

Excepciones:

Salidas:

Precondiciones: Que se el cliente este registrado en la tarjeta de registro

Postcondiciones: Actualizar los datos de la Tarjeta de Registro con los datos de salida del cliente

7.- Gestionar Usuarios

Diagrama de Secuencia

FIGURA V-31. DIAGRAMA DE SECUENCIA GESTIONAR USUARIOS

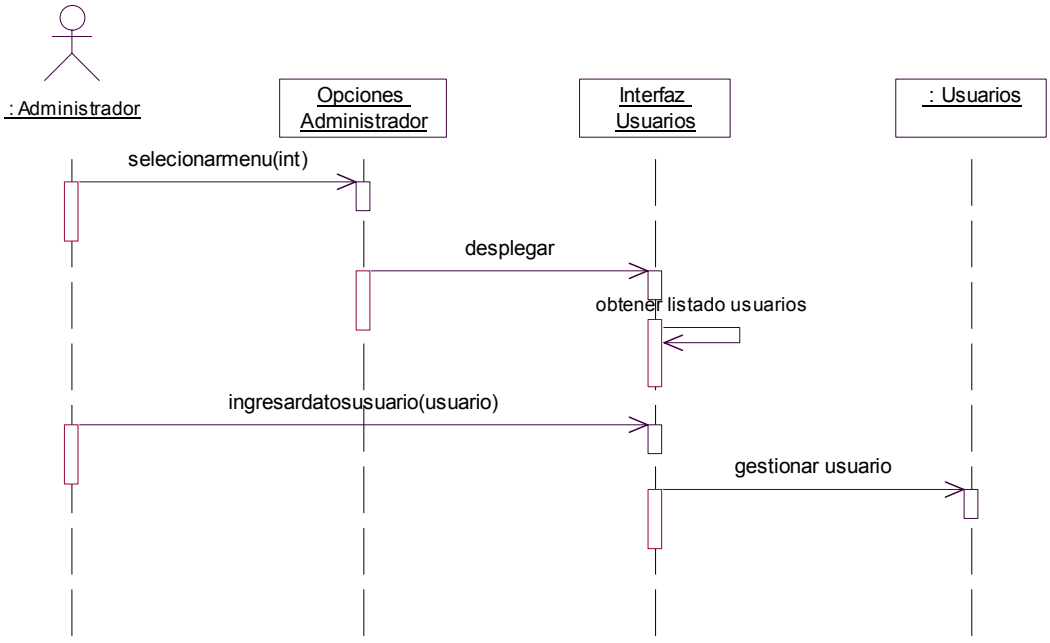
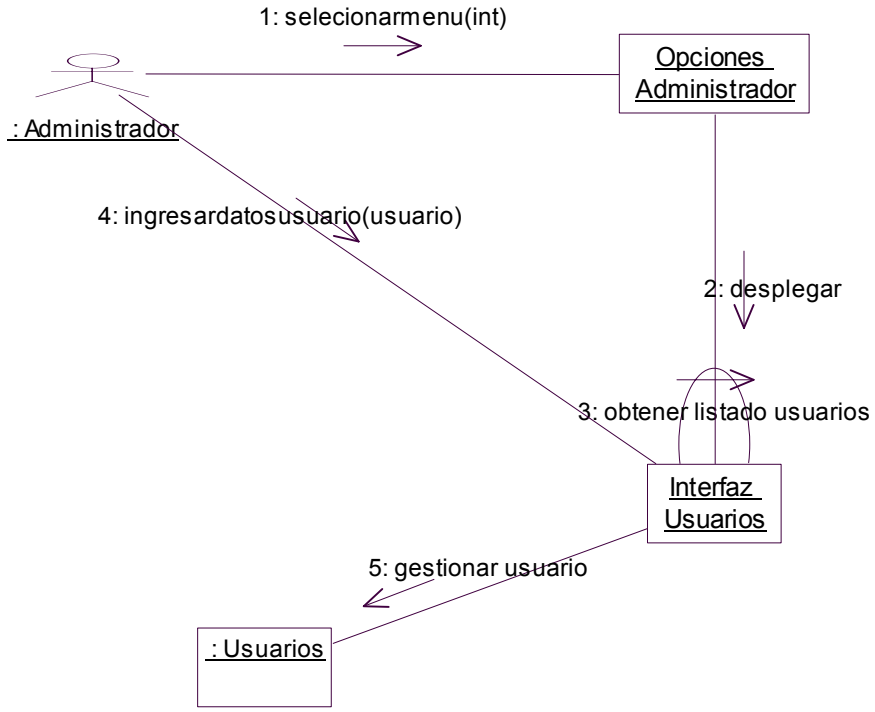


Diagrama de Colaboración

FIGURA V-32. DIAGRAMA DE COLABORACIÓN GESTIONAR USUARIOS



Contrato de Operación

Nombre: gestionarusuario(usuario):boolean

Responsabilidad: Permite gestionar un nuevo usuario del sistema puede ser de dos tipos administrador o operario esto depende del perfil que se especifique

Tipo: Usuario

Caso de Uso: Gestionar Usuarios

Notas:

Excepciones:

Salidas:

Precondiciones: Debe de estar previamente registrados los permisos

Postcondiciones: Un nuevo objeto usuario es creado

8.- Gestionar Llamadas Telefónicas

Diagrama de Secuencia

FIGURA V-33. DIAGRAMA DE SECUENCIA GESTIONAR LLAMADAS TELEFÓNICAS

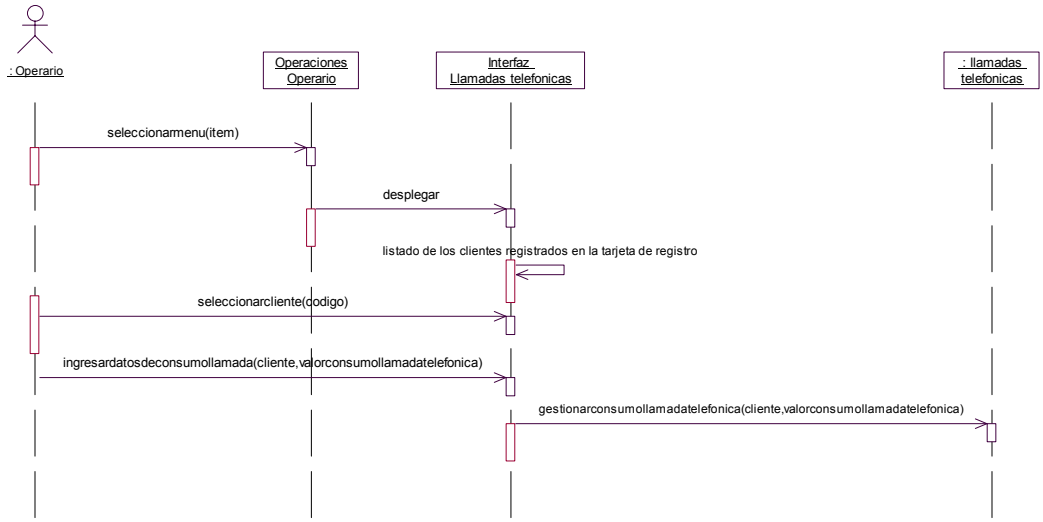
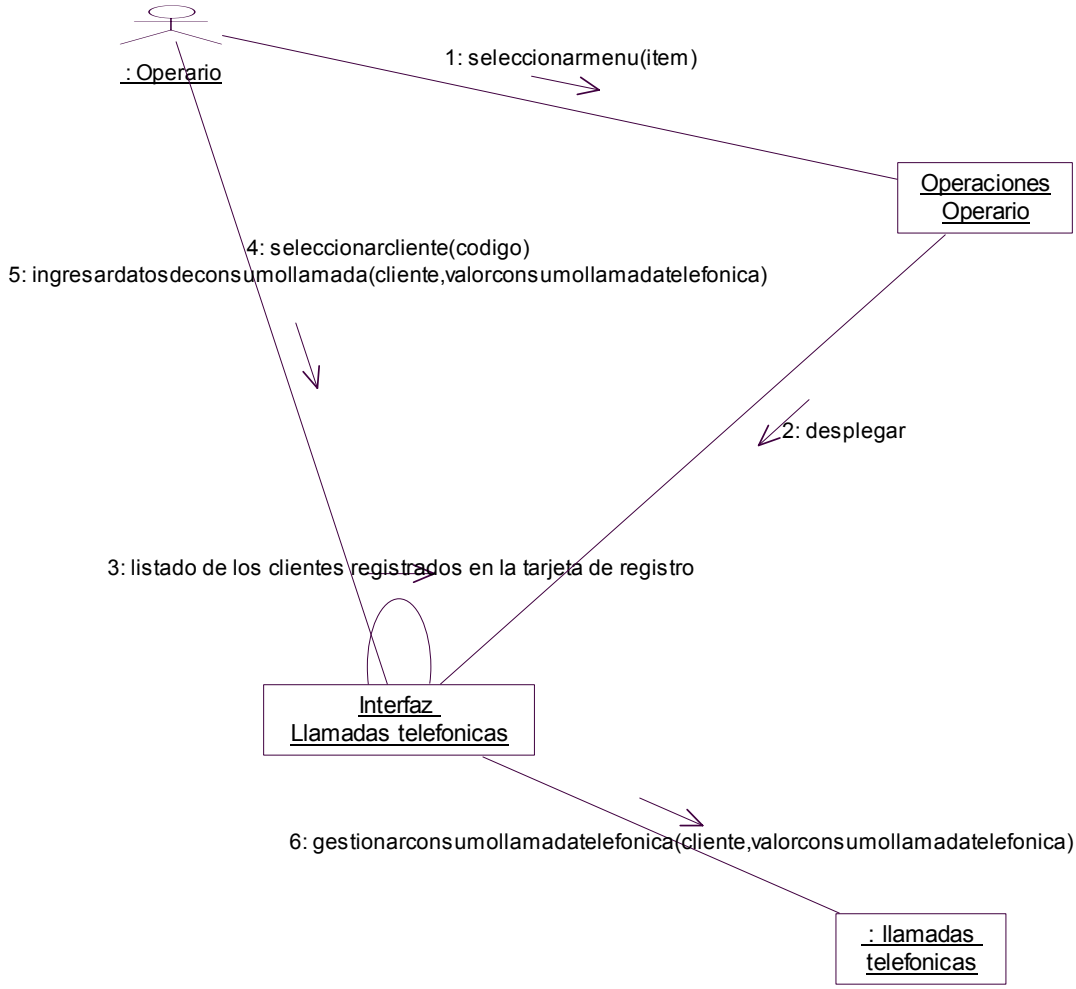


Diagrama de Colaboración

FIGURA V-34. DIAGRAMA DE COLABORACIÓN GESTIONAR LLAMADAS TELEFÓNICAS



Contrato de Operación

Nombre: gestionarllamadastelefonicas(cliente,consumollamadatelefonica):boolean

Responsabilidad: Permite gestionar los consumos de las llamadas telefónicas en los que incurren el cliente durante su estadía en el Hotel

Tipo: Reservación

Caso de Uso: Gestionar Llamadas telefónicas

Notas:

Excepciones:

Salidas:

Precondiciones: Que se el cliente este registrado en la tarjeta de registro

Postcondiciones: Un objeto consumo llamada telefónica se ha creado

9.- Gestionar Gastos

Diagrama de Secuencia

FIGURA V-35. DIAGRAMA DE SECUENCIA GESTIONAR GASTOS

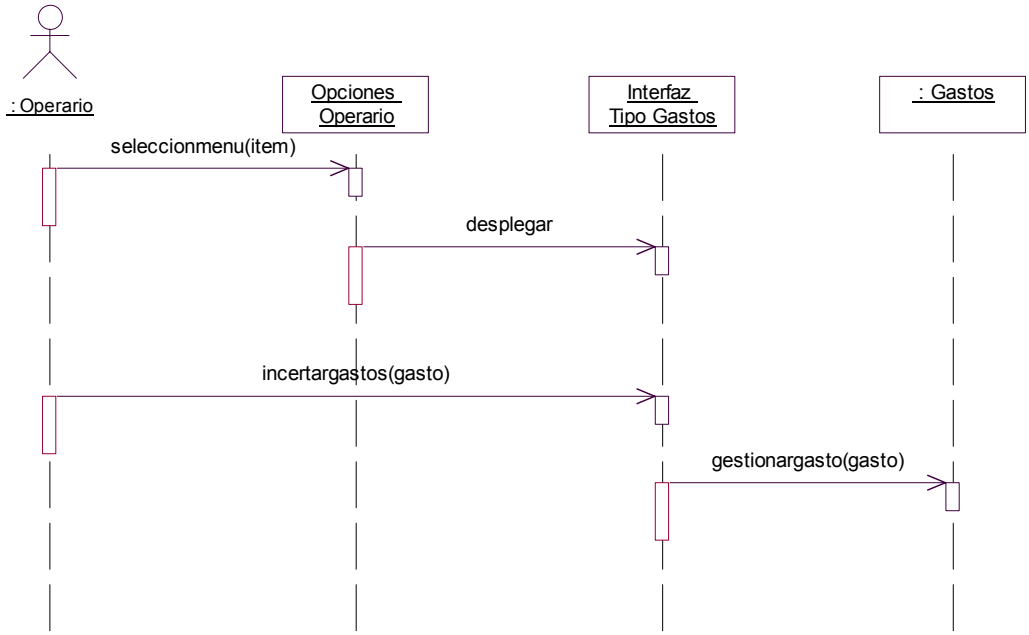
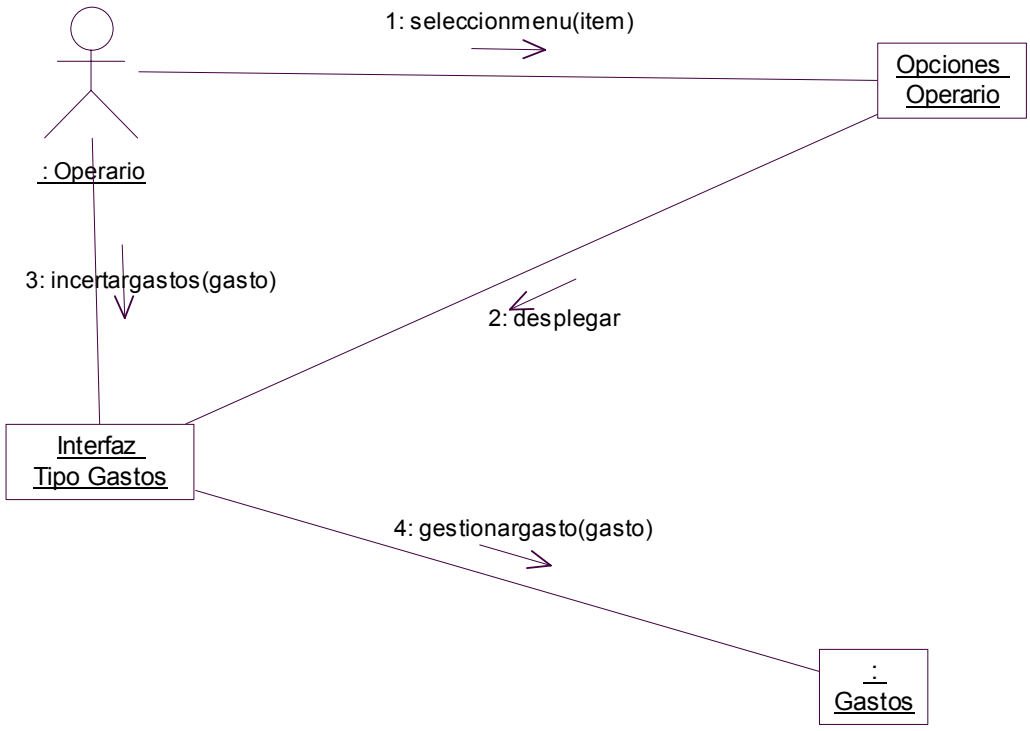


Diagrama de Colaboración

FIGURA V-36. DIAGRAMA DE COLABORACIÓN GESTIONAR GASTOS



Contrato de Operación

Nombre:gestionargastos(gasto):boolean

Responsabilidad: Permite gestionar los gastos que realiza el hotel, cada gasto se realiza en base a un centro de costo, los datos requeridos para cada ingreso de gastos son los siguientes fecha, cantidad, valor, forma de pago, y una breve descripción del gasto

Tipo: Gasto

Caso de Uso: Gestionar Gastos

Notas:

Excepciones:

Salidas:

Precondiciones: Tener Registrados los centro de costos para poder gestionar gastos

Postcondiciones: Un objeto gasto es creado

10.- Gestionar Consumos

Diagrama de Secuencia

FIGURA V-37. DIAGRAMA DE SECUENCIA GESTIONAR CONSUMOS

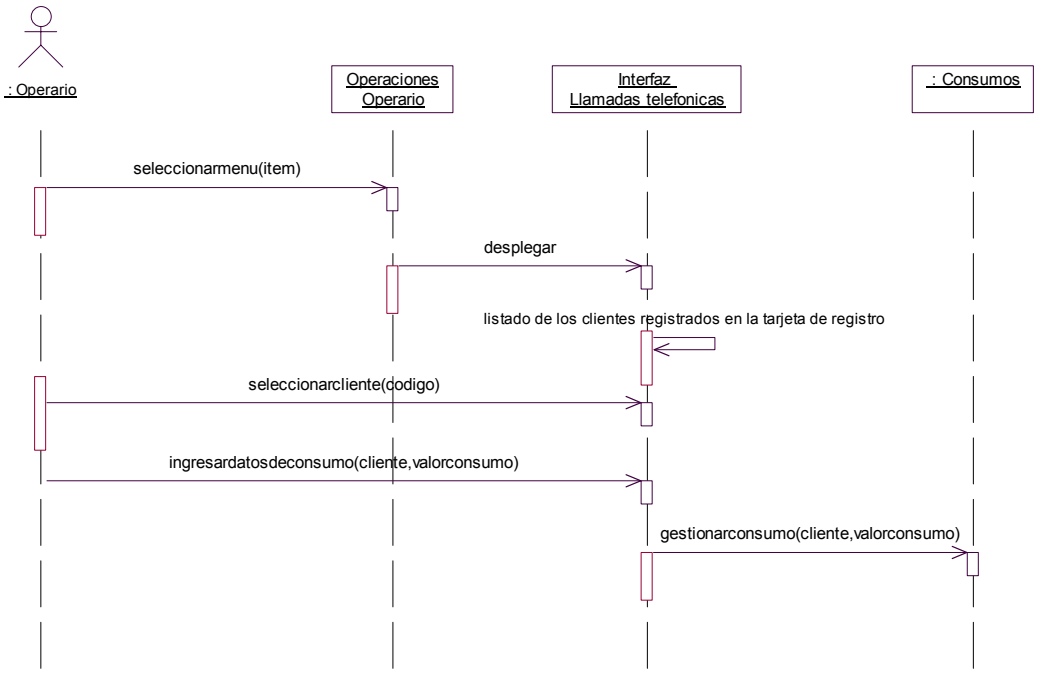
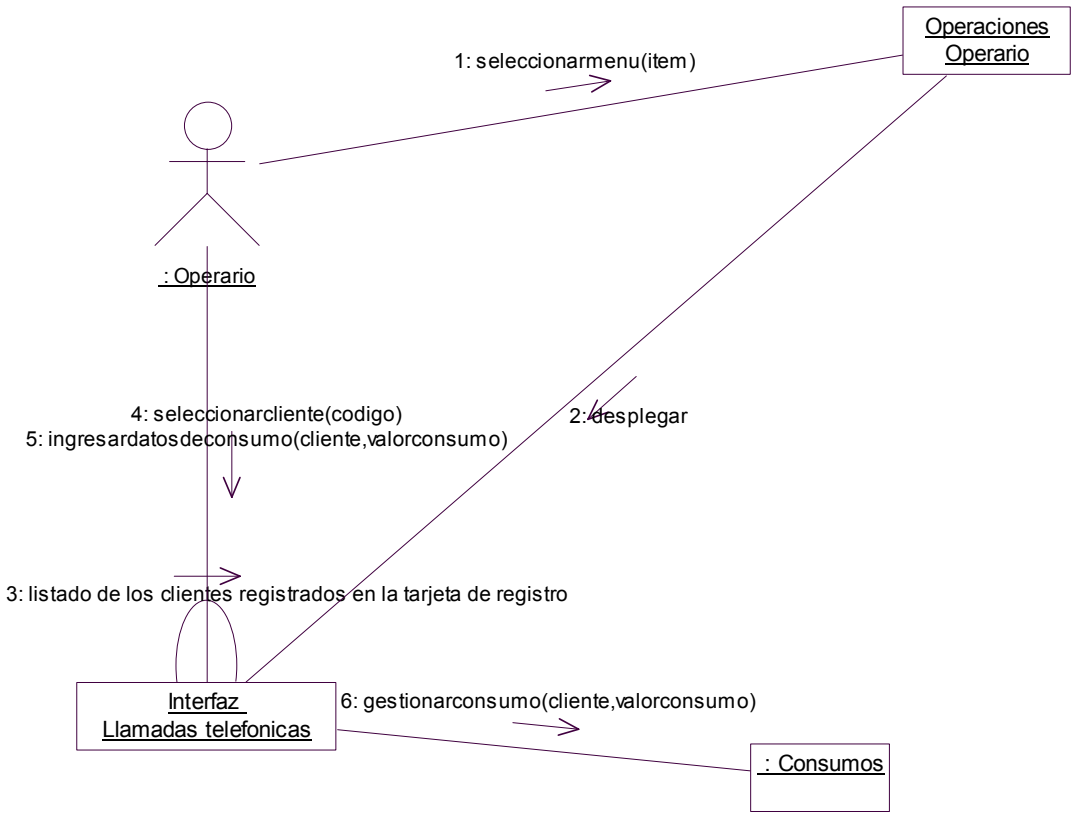


Diagrama de Colaboración

FIGURA V-38. DIAGRAMA DE COLABORACIÓN GESTIONAR CONSUMOS



Contrato de Operación

Nombre: gestionarconsumos(cliente,consumo):boolean

Responsabilidad: Permite gestionar los consumos en los que incurren el cliente durante su estadía en el Hotel

Tipo: Reservación

Caso de Uso: Gestionar Consumos

Notas:

Excepciones:

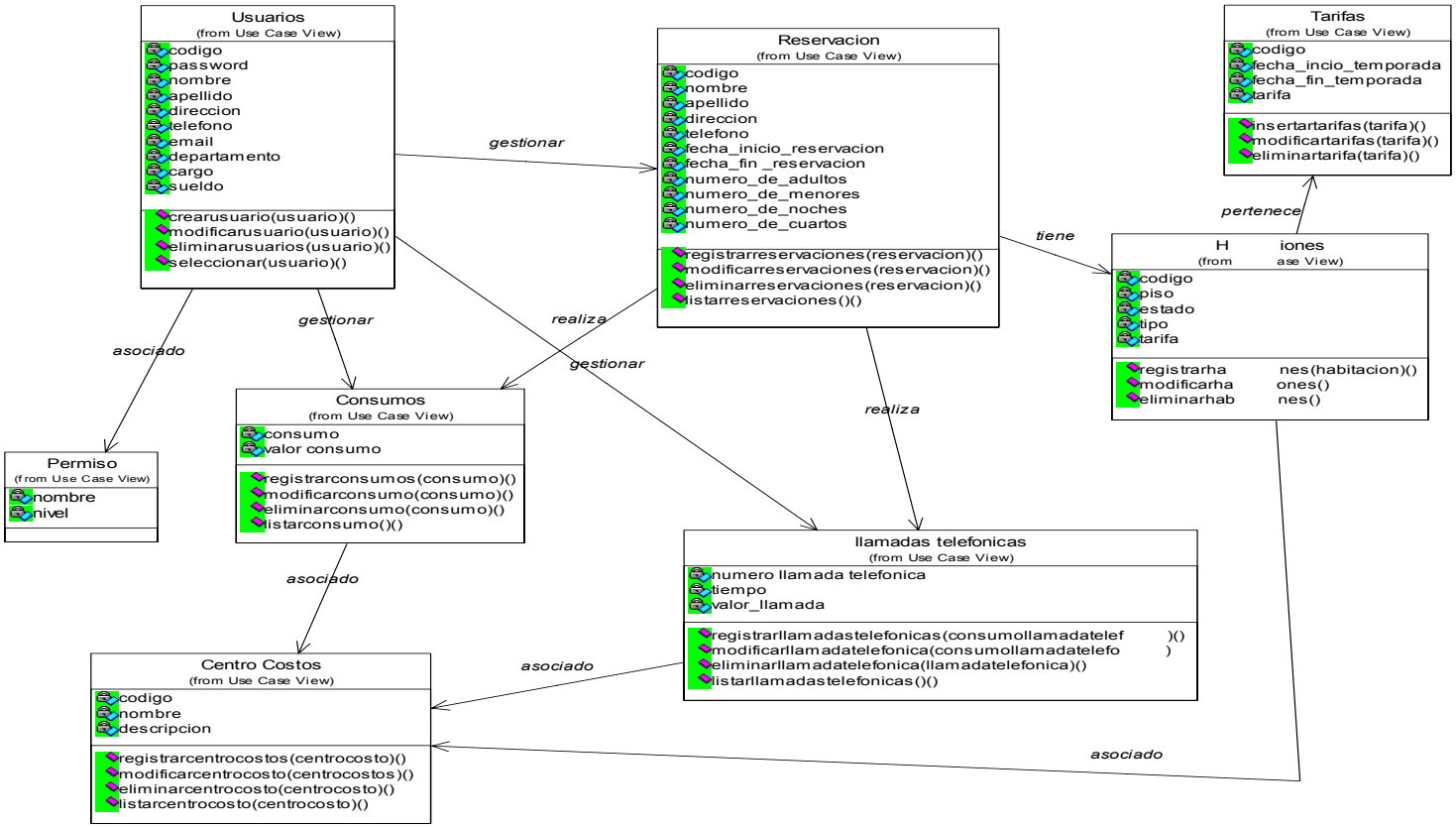
Salidas:

Precondiciones: Que se el cliente este registrado en la tarjeta de registro

Postcondiciones: Un objeto consumo se ha creado

5.2.2.1.- Diagramas de Clases

FIGURA V-39- DIAGRAMA DE CLASES DEL SISTEMA



Capitulo

6

VI. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones a las cuales se ha llegado luego de haber realizado un estudio de las ventajas que brinda un ASP y la manera de implantarlo con herramientas Open Source.

6.1.- CONCLUSIONES

- Los ASP agrupan servicios permitiendo a los clientes interactuar con un solo punto de contacto y no con una colección de tecnologías y proveedores.

- Un ASP realmente es una opción que deben tener presente las empresas en estos días en los cuales los avances en temas de TI son muy frecuentes, las empresas no se pueden dar el lujo de cambiar de tecnología cada 6 meses, por lo cual más factible resulta contratar los servicios de un tercero en este caso un ASP que se preocupe de estos temas.

- Con una solución ASP se reduce significativamente el tiempo y costo de la fase de implementación o en muchos casos casi es nula, porque a la misma aplicación la estoy compartiendo para que varios clientes la usen .

- Con un modelo ASP ya no es necesario realizar una gran inversión para poder acceder a aplicaciones complejas, básicamente el usuario solo debe tener un browser y acceso a la aplicación.

- Cuando una empresa realiza inversiones de software, tiene que pensarlo muy bien antes de comprar un sistema, puesto que si luego de realizada la compra y terminada la garantía el sistema no cumple con los requerimientos de la empresa se habrá perdido la inversión, bajo un modelo ASP las empresas pueden probar las aplicaciones, muchas veces gratis, otras por un pago muy irrisorio y en el instante que la empresa esté segura que ese sistema cumple con todos los requisitos, se pasa a la fase de contrato con el ASP, como en este modelo el cliente solo paga por el uso de la aplicación en cualquier momento podrá terminar el contrato con el ASP pudiendo de esta manera salvar su inversión.

- Las empresas ya no tienen que comprar hardware de última tecnología o especializado para poder acceder a sus aplicaciones, basta con contratar un ASP el cual se ocupará de brindar este tipo de tecnología .

- La piedra angular en Internet es la seguridad, es un tema bastante árido en el cual muchos opinan pero como en el mundo real nadie esta seguro, la tecnología SSL de encriptación de datos es una muy buena alternativa a mas de ser la mas barata, esta tecnología tiene las características de encintar los datos a 128 bits asincrónicamente, con firma digital lo que hace *que el dominio que dice ser sea en verdad el dominio que dice ser*, dando a los cliente total tranquilidad al momento de enviar sus datos .

- Muchas de las veces se debe realizar un estudio de la aplicación puesto que si esta funciona de manera exitosa en el modelo tradicional, tal vez no lo hará de la misma manera al volcarlo en el modelo ASP por lo que habrá que rediseñar la aplicación.

- Dentro de los servicios que un ASP debe brindar es la fácil migración de datos a cualquier base, este servicio permitirá al cliente poder subir los datos al ASP y en el momento que el cliente desee migrar sus datos a otra aplicación lo pueda realizar de manera transparente.

- Con el modelo ASP se puede proveer las aplicaciones a cualquier parte del mundo sin que el técnico se traslade físicamente, él solo provee de un acceso al cliente, y el cliente a través de Internet o una red privada puede accede a la aplicación .

6.2.- RECOMENDACIONES

- Aunque en esta tesis el objetivo ha sido la implementación de un ASP con herramientas de libre difusión, no hay que olvidar que existe el otro tipo de herramientas, las que tiene copyright y tienen su costo, mas aun un ASP debe proveer de las facilidades suficientes para satisfacer a los clientes, un ejemplo de ello es DATADEC esta empresa presenta una tecnología de desarrollo e implementación Open Source por un lado y por el otro y en paralelo presenta tecnologías con copyright, por ejemplo su sistema operativo es Windows 2000 y su base de datos Oracle, es decir el ASP tiene varias ofertas.

- Una de los tópicos que las personas suelen olvidar son las seguridades físicas, en un ASP es una de las partes que mas hay que tomar en cuenta , todos los ASP serios en el mundo, en primera instancia tienen un infraestructura antisísmica, con censores de humedad, temperatura y extintores de incendios especializados para proteger los equipos de computo.

- No solo las seguridades físicas son importantes, hay otras que tiene mucha mayor probabilidad de ocurrencia como son los ataque por infiltración en la red o en el centro de datos, para la primera su solución mas rápida de implantar y barata es instalar un Firewall vía software y para la segunda existen variadas opciones desde una simple tarjeta hasta un reconocedor biométrico en 3D, todo depende del tipo de datos que este a su cargo y los recursos que posea el ASP, una de las opciones baratas y fácil sería el

cerrar bajo llave el centro de datos del ASP cuando ninguna persona autorizada se encuentre.

- La principal recomendación al momento de escoger el hardware para la implantación de un ASP es que sea escalable es decir que se puede actualizar en cualquier instante nuestro ASP que tiene actualmente 100 clientes debe prever capacidad y disponibilidad para soportar a 200 clientes mas en cualquier momento, una de las términos que utilizan los expertos de los ASP es que el sitio debe llegar a ser 'self-sufficent' (auto-suficiente).

- Como dice el adagio "divide y vencerás", se debe de contar con partners tecnológicos líderes a nivel mundial; como es normal el avance tecnológico se encaminan a los objetivos de los líderes tecnológicos tales como Microsoft, Oracle, IBM, Compaq, entre otros, un ASP debe de realizar convenios con estos líderes para poder estar siempre a la vanguardia de la tecnología y poder servir de mejor manera a los clientes.

- Antes de crear una nueva aplicación para que funcione en el modelo ASP se debe realizar un estudio de mercado, para poder recuperar la inversión realizada en el desarrollo de la aplicación, además cabe resaltar que no todas las aplicaciones que trabajan bien en un modelo tradicional trabajaran de la misma manera en un modelo ASP, muchas de estas aplicaciones deben ser rediseñadas.

- Uno de los servicios que un ASP debe brindar es la actualización periódica de las aplicaciones, no hay que olvidar que sin clientes la aplicación no tiene razón de ser .

- La redundancia no es más que tener dos o mas ASP que tengan lo mismo es decir una analogía a lo que tiene Windows NT con su Mirror, cuando el dominio primario se cae el dominio de respaldo pasa a ser el primario hasta que el primario se restablezca, este termino no solo es utilizado en ASP o

centros de computo, la Marina de los Estados Unidos utilizan redundancia con sus submarinos atómicos.

- Los datos es la parte mas importante sistema computacional, el Hardware se puede recuperar, el Software se puede volver a instalar pero los datos muchas de las veces es imposible de recuperar es aquí cuando aparece la necesidad de realizar copias de respaldo de datos, en un ASP se debe tener un calendario muy frecuente y riguroso de ejecución del proceso de copias de respaldo en caliente.

- Otra recomendación importante es la disponibilidad que debe brindar un ASP, para el cliente debe ser muy transparente que la aplicación está a cientos de kilómetros, el cliente solo tendrá la percepción que la aplicación se esta ejecutando en su misma máquina .

- Puesto que un ASP provee aplicaciones la mayoría de las veces vía Internet es muy importante el encriptar los datos sensibles al envío y recepción, de esta manera el cliente podrá estar un poco mas tranquilo

Anexo

A

IMPLANTACIÓN DE UN ASP(APPLICATION SERVICE PROVIDER) ORIENTADO A LA HOTELERIA Y TURISMO

Referencia Bibliográfica

ANEXO A: REFERENCIA BIBLIOGRAFICA

NOTICIAS RESPECTO A LAS EMPRESAS QUE BRINDAN SERVICIOS COMO ASP
www.aspnews.com

EMPRESA DEDICADA AL MONITOREO DE LA TECNOLOGÍA QUE USAN LOS DOMINIOS DE INTERNET
www.netcraft.com

AUTORIDAD CERTIFICADORA
www.verisign.com

PROYECTO PHP
www.php.net

LINUX RED HAT
www.redhat.com

PROYECTO MYSQL
www.mysql.com

PROYECTO APACHE
www.apache.com

PROYECTO MIDGARD
www.midgard-project.org

PROYECTO SSL
www.openssl.org

SEGURIDADES EN SERVIDORES PARA INTERNET

www.rediris.es

DIRECCIONES VARIAS DE REFERENCIA

EMPRESA ASP ARGENTINA

www.cabase.org.ar

EMPRESA ASP URUGUAYA

www.interempresa.com/asp/

OUTSORCING

www.bull.es/servicio/oper21_a.htm

ECOMMERCE

www.mexicoextremo.com.mx/ayuda/robo-info-ecommece.php

Anexo

B

Acrónimos

ANEXO B: ACRÓNIMOS

ACRÓNIMO	DESCRIPCIÓN
24*7	DISPONIBILIDAD 24 HORAS * 7 DIAS A LA SEMANA
ALLASP	ORGANIZACIÓN PRINCIPAL DE LOS ASP
ANDINATEL	EMPRESA DE SERVICIO TELEFÓNICOS
APPLICATION SERVER	SERVIDOR DE APLICACIONES
ASP	SERVIDOR DE SERVICIOS DE APLICACIÓN
ASP INTEGRA	EMPRESA QUE BRINDA SERVICIO DE ASP EN ESPAÑA
B2B	BUSINESS TO BUSINESS COMMERCE
B2C	BUSINESS TO COMMERCE
CA	AUTORIDAD CERTIFICADORA
CERT	COMPUTER EMERGENCY RESPONSE TEAM
CERTIFICADO DIGITAL	DOCUMENTO DE IDENTIFICACIÓN USADO EN EL INTERNET
CGI	COMMON GATEWAY INTERFACE
CHECK IN	REGISTRO DE ENTRADA A CLIENTES
CHECK OUT	REGISTRO DE SALIDA DE CLIENTES
CORE BUSINESS	NEGOCIO PRINCIPAL DE LA EMPRESA
CRM	CUSTUMER RELATIONSHIP MANAGEMENT
DARPA	DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
DATA BASE SERVER	SERVIDOR DE BASE DE DATOS
DATADEC	EMPRESA ASP ESPAÑOLA
E-BUSINNESS	NEGOCIO ELECTRÓNICO
E-COMMERCE	COMERCIO ELECTRÓNICO

FIREWALLING	POLÍTICAS DE RESTRICCIÓN DE ACCESO
HOSTING	HOSPEDAJE
HOTELMATIC	SISTEMA HOTELERO
HTTP	PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO
I+D	INVESTIGACIÓN Y DESARROLLO
IDC	EMPRESA ENCARGADA DE REALIZAR ANÁLISIS DE TECNOLOGÍA
INTRÍNSECA	ACTIVIDAD PURA
IRC	INTERNET RELAY CHAT
ISP	PROVEEDOR DE INTERNET
MIDGARD	SERVIDOR DE APLICACIONES
NFS	SISTEMA DE ARCHIVOS DE RED
PHP	PRE - PROCESADOR DE HIPERTEXTO
PYMES	PEQUEÑA Y MEDIANA EMPRESA
RAS	SERVICIO DE ACCESO REMOTO
REDUNDANCIA	DUPLICACIÓN DE TECNOLOGÍA PARA CUIDAR LA DISPONIBILIDAD
SAI	SERVICIO DE ALIMENTACIÓN ININTERRUMPIDA
SET	TRANSACCIONES ELECTRÓNICAS SEGURAS
SGDB	SISTEMA DE GESTION DE BASE DE DATOS
SNIFFERS	PROGRAMAS CAPTURADOTES DE PAQUETES TCP USADO POR LOS HACKERS
SSL	CAPA DE CONEXIÓN SEGURA
TCP	PROTOCOLO DE TRANSFERENCIA
TI	TECNOLOGÍA DE LA INFORMACIÓN
UML	LENGUAJE DE MODELADO UNIFICADO
URL	LOCALIZACIÓN UNIFORME DE RECURSO
VPN	REDES DE ÁREA EXTENDIDA
WAN	REDES DE ÁREA MUNDIAL
WEB BROWSER	PROGRAMA PARA NAVEGAR EN INTERNET

WEB SERVER	SERVIDOR DE INTERNET

Anexo

C

IMPLANTACIÓN DE UN ASP(APPLICATION SERVICE PROVIDER) ORIENTADO A LA HOTELERIA Y TURISMO

Manual de Usuario del Sistema

ANEXO C: MANUAL DE USUARIO DEL SISTEMA

PARA REVISAR EL MANUAL DE USUARIO DEL SISTEMA REFIERASE AL CD DE HOTELMATIC

BAJO DE LA CARPETA USUARIO_MANUAL

Anexo

D

IMPLANTACIÓN DE UN ASP(APPLICATION SERVICE PROVIDER) ORIENTADO A LA HOTELERIA Y TURISMO

Manual Técnico del Sistema

ANEXO D: MANUAL TÉCNICO DEL SISTEMA

PARA REVISAR EL MANUAL TECNICO DEL SISTEMA REFIERASE AL CD DE HOTELMATIC

BAJO DE LA CARPETA TECNICO_MANUAL

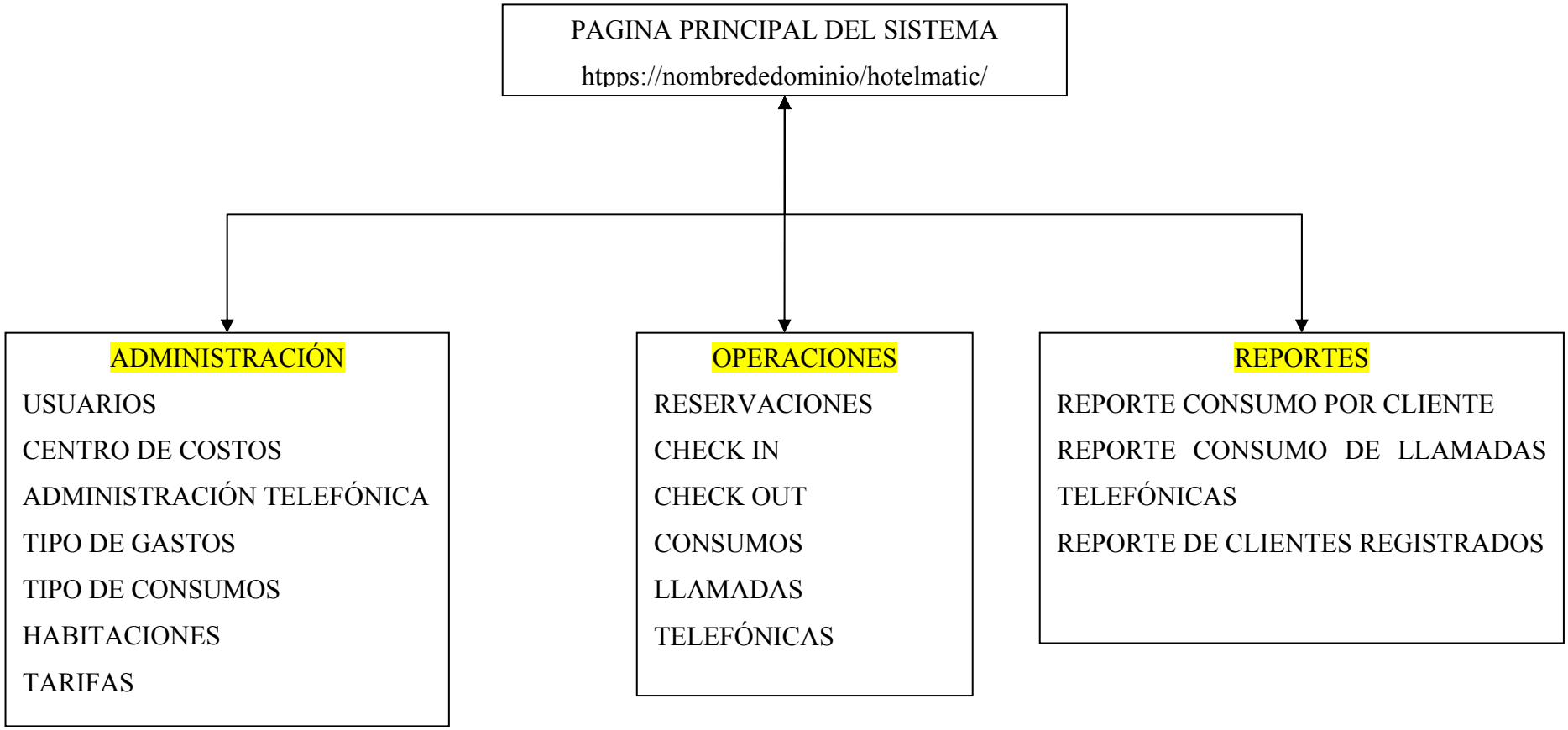
Anexo

E

Interfaces del Sistema

ANEXO E INTERFACES DEL SISTEMA

Figura D-1 Diagrama de Interfaces del Sistema



Anexo

F

IMPLANTACIÓN DE UN ASP(APPLICATION SERVICE PROVIDER) ORIENTADO A LA HOTELERIA Y TURISMO

Interfaces de Herramientas

ANEXO F: INTERFACES DE HERRAMIENTAS

Figura F-1 Diagrama de Interfaces de Herramientas