ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Sitio electrónico de pagos y transferencias en línea: Análisis, Diseño e Implementación de Sistema de Pagos y Transferencias en línea, aplicado a Sitios de Comercio Electrónico en Internet"

TRABAJO DE GRADUACIÓN

Previa a la obtención del título de:

INGENIERO EN COMPUTACIÓN

ESPECIALIZACIÓN SISTEMAS TECNOLÓGICOS

Presentada por:

PETER E. CALDERÓN PONCE
LUIS FERNANDO RUIZ VERA
ROMINA YÉPEZ PÉREZ

GUAYAQUIL – ECUADOR
2005

AGRADECIMIENTO

A Dios, a nuestros padres, compañeros, amigos y a todas aquellas personas que nos brindaron el apoyo necesario para la producción de este trabajo.

Gracias al Centro de Servicios Informáticos, a la directora MBA. Ruth Álvarez, por su apoyo incondicional y sus miembros.

TRIBUNAL DE GRADUACIÓN

Ing. Miguel Yapur
Subdecano de la Facultad de Ingeniería en Electricidad y Computación

Ing. Karina Astudillo
Director de Tópico

Ing. Guido Caicedo
Miembro del Tribunal

Ing. Marcelo Loor
Miembro del Tribunal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la: Escuela Superior Politécnica Del Litoral"

(Reglamento de Graduación de la ESPOL).

Peter Calderón	Luis F. Ruiz V.	Romina Yépez

RESUMEN

El presente proyecto permite una solución favorable a muchos usuarios que acceden a múltiples sitios de comercio electrónico al realizar sus compras a través del Internet de manera segura, confiable y rápida.

El usuario podrá contar con un único acceso de sus datos personales y de tarjetas de crédito o cuentas bancarias a través de este sistema de pagos electrónicos en línea, de tal manera que cuando el usuario desea realizar una transacción comercial en algún sitio de comercio electrónico, simplemente agregue su único usuario como es, el correo electrónico personal e intransferible, en el sitio afiliado al sistema de pagos electrónicos y automáticamente se realizan las respectivas transferencias entre el cliente y el proveedor del producto.

Para esto, tanto el usuario final, el que desea comprar, como el usuario comercial, es decir, la empresa que desea vender sus productos por un sitio de comercio electrónico, deben registrarse en nuestro sistema de pagos y especificar la información pertinente a cuentas bancarias y tarjetas de crédito, para realizar las transferencias respectivas.

Para realizar tal tarea, proponemos un diseño e implementación de la infraestructura de la red y del sitio Web de pagos electrónicos considerando que se han aplicado los principales principios de seguridad, tales como:

- Confidencialidad
- Autenticidad
- Privacidad
- Integridad

Además se han considerando técnicas de tolerancia a fallos, diseño en capas, sistemas de firewalls, sistemas de detección de intrusos, contingencias, conexiones seguras. De esta manera, mantener a este servicio en línea el mayor tiempo posible, y evitar posibles ataques de hackers.

Funcionalmente el sistema de pagos, permitirá realizar al usuario operaciones como registro de cuentas bancarias o tarjetas de crédito, envío de dinero, recepción de dinero, consulta de movimientos y actualización de datos personales y de cuentas, facilitando así al usuario realizar las tareas más requeridas.

Algunas de estas opciones están disponibles para tanto los usuarios naturales como los empresariales que desean afiliarse a nuestro sitio para facilitarle al usuario la transferencia de su dinero de manera segura.

Estas transferencias se realizaran mediante comunicaciones seguras entre nuestros servidores y los equipos y servidores de las instituciones financieras.

De tal manera que siempre el usuario mantendrá actualizada su información en nuestro sistema de pagos electrónicos, como en sus cuentas bancarias o tarjetas de crédito.

Siempre será nuestra prioridad brindar el servicio durante todo el día, y mantener la seguridad de las comunicaciones, ya que una posible falla en nuestro sitio, es decir, que el sitio esté fuera de línea durante poco o mucho tiempo, representa pérdidas financieras, y molestias al usuario, porque en ese tiempo no se podría realizar transacciones en línea.

ÍNDICE GENERAL

PAG.

ÍNDICE DE FIGURAS

PAG.

ÍNDICE DE TABLAS

PAG.

ÍNDICE DE ABREVIATURAS

ACL	Access Control List
ASP	Active Serve Pages
DIDS	Distributed Intrusion Detection Systems
EDI	Electronic Data Interchange
HIDS	Host Intrusion Detection Systems
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IDS	Intrusión Detection Systems
IMAP	Internet Messages Access Protocol
IKE	Internet Key Exchange
IPSEC	IP Security
IVE	Instant Virtual Extranet
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
NAT	Network Address Translation
NFS	Network Files System

NIC	Network Interface Card
PC	Personal Computer
PHP	Hypertext Preprocessor
POP	Post Office Protocol
RAM	Random Access Memory
RPC	Remote Procedure Call
SKIP	Simple-Key Management for Internet Protocols
SMTP	Single Mail Transfer Protocol
SSL	Secure Socket Layer
UTP	Unshield Twisted Pair
VPN	Virtual Private Networks
XML	Extensible Markup Language

INTRODUCCIÓN

El presente documento tiene como finalidad mostrar la documentación del análisis, diseño, e implementación del Sitio electrónico de pagos y transferencias en línea, basado en técnicas de seguridades de información aplicadas a Internet.

Este Sistema fue desarrollado como uno de los proyectos del tópico de graduación “Seguridad de la información”, previo a la obtención del título de Ingeniero en Computación.

El “Sitio electrónico de pagos y transferencias en línea” es el resultado de incorporar las técnicas de análisis, diseño e implementación, formadas en el transcurso de la carrera, así como las técnicas de seguridades aprendidas en la exposición del tópico de Seguridades de Información.

Para el desarrollo del “Sitio electrónico de pagos y transferencias en línea”, se tuvo que investigar sobre sitios en Internet con servicios parecidos a los que requeríamos implementar, y de estos, investigar y conocer un poco más sobre la lógica del negocio y las funcionalidades del sitio.

Para un mejor conocimiento del proyecto, se han documentado 6 capítulos, en los cuales se detalla cada etapa del proyecto:

- Capítulo I, se proporcionará la descripción del problema, el enfoque a la necesidad y la justificación de un Sitio electrónico de pagos y transferencias en línea. Se indicaran el objetivo general y los objetivos específicos, así como los alcances y las limitaciones del Sistema.

- Capítulo II, se expondrá un análisis de mercado para un sistema de pago electrónico, las necesidades y los servicios a implementarse, el segmento de mercado y la competencia.

- Capítulo III, se mostrará los mecanismos empleados para la infraestructura de red implementada, las políticas y sus respectivos diseños de red.

- Capítulo IV, se detallará los mecanismos se seguridad implementados, incluyen firewalls, IDS, Antivirus, Correo Electrónico, Seguridad de Base de datos, Seguridad de Servidores.

- Capítulo V, se detallara, el análisis, diseño del Sitio electrónico de pagos y transferencias en línea, así como sus herramientas tecnológicas para su implementación

- Conclusiones y recomendaciones.

CAPÍTULO I

INTRODUCCIÓN

1.1 Definición del problema y justificación del proyecto

En este capítulo se presenta la descripción del problema y la necesidad que se observó para el desarrollo del Sitio electrónico de pagos y transferencias en línea, el cual tiene como nombre PagoSeguro. Se indicarán los objetivos, justificaciones, alcances y limitaciones del mismo.

Junto con el crecimiento de Internet han surgido los Sitios de comercio electrónico, ofreciendo todo tipo de productos en línea, sin embargo, los consumidores siguen siendo evasivos a esta nueva forma de adquisición, por la inseguridad que sienten al realizar transacciones o compras en línea, debido a que una de las formas de pago más utilizadas en Internet es el cargo a tarjetas de crédito y por tanto son víctimas de fraudes.
Además planteamos una alternativa de envío de dinero desde el exterior para muchas personas ecuatorianas residentes fueran de nuestro país, de manera confiable y segura.

Comprar en Internet, puede ser tan seguro como inseguro, actualmente sabemos lo común que es el fraude en Internet y cómo los hackers se apropian de los números de tarjetas de crédito con una y mil técnicas

informáticas, en ese contexto, y si nos guiáramos exclusivamente por la opinión mayoritaria, lo pensaríamos dos veces antes de introducir los números de las cuentas bancarias o tarjetas de créditos en un formulario de un sitio web.

Además, cuando se realizan compras en Internet, casi siempre se adquieren productos de más de un sitio, promoviendo a la propagación masiva de la información financiera en Internet, lo cual aumenta el riesgo de fraude.

De lo anterior expuesto, se resume que el inconveniente de realizar comercio electrónico en Internet, es la seguridad que con la que se debe administrar los datos personales y más aún los financieros.

Dar la certeza al comprador, y al que envía dinero desde el exterior mediante transferencias, de que es un sitio seguro al cual se le está proporcionando la información, y evitar que el comprador tenga que proporcionar varias veces la información financiera en Internet.

La solución que nosotros planteamos e implementamos, fue desarrollar un Sitio electrónico de pagos y transferencias en línea, en el cual los usuarios registrados pueden enviar un pago a cualquier persona con una dirección de correo electrónico, con sólo escribir una cantidad en dólares en un formulario

en línea. Cuando se envía el correo electrónico, el pago se cobra a la tarjeta de crédito o cuenta bancaria del remitente.

El registro del usuario, es sencillo y rápido; los procedimientos de PagoSeguro corroboran que los datos del registro sean fiables y confirmados por el usuario. Una vez realizado este proceso el usuario ya tiene una cuenta en PagoSeguro, pero debe definir los datos financieros, como número de cuenta bancaria y/o de tarjeta de crédito para que pueda enviar y recibir dinero.

Los datos financieros proporcionados por el usuario son registrados bajo una conexión segura con PagoSeguro, y son proporcionados una sola vez, de esta manera se protege al usuario de propagar sus datos financieros a través de Internet, y los pagos de las compras y/o cobros que él realice, se harán por medio de PagoSeguro.

Los usuarios pueden decidir dejar su dinero en su cuenta de PagoSeguro, para volverlo a usar, pero este no devengará intereses. También el usuario podrá elegir retirar el dinero de PagoSeguro y transferirlo a su cuenta bancaria o a su tarjeta de crédito.

El mantenimiento de la cuenta en PagoSeguro, es gratis, pero las transferencias a cuentas bancarias de los usuarios sí tienen costo.

1.2 Objetivo general

El objetivo macro de PagoSeguro es permitir a cualquier negocio o consumidor, con una dirección de correo electrónico, poder enviar y recibir pagos en línea con seguridad, eficacia y a bajo costo; todo esto por medio de PagoSeguro el cual provee una interfaz grafica basada en Web, amigable y de fácil uso. Facilitar a los usuarios de PagoSeguro, el uso de los servicios del mismo.

1.2.1 Objetivos especificos

- Permitir que una persona natural o jurídica que tenga una dirección de correo electrónico, pueda registrarse y formar parte de los usuarios de PagoSeguro.

- Ingreso único de la información financiera (Números de Tarjetas de Crédito y/o Cuentas Bancaria) del usuario en PagoSeguro.

- Proporcionar la seguridad técnica y física para la administración de los datos personales y financieros de los usuarios, así como de las transacciones que efectúe.

- Permitir realizar pagos entre los sitios de comercio electrónico y los usuarios, uno y otro registrados en el PagoSeguro.

- Permitir realizar pagos entre sitios de comercio electrónicos registrados.

- Permitir efectuar aumento de saldo a la cuenta virtual del usuario registrado en PagoSeguro, por medio de transferencias, con débito de los valores a las cuentas bancarias o tarjetas de crédito del usuario.

- Permitir efectuar transferencias de dinero de la cuenta virtual del usuario en PagoSeguro, a las cuentas bancarias o tarjetas de crédito del usuario.

- Permiter el envío de dinero a usuarios desde fuera del país hacia sus familiares en el Ecuador, a través de una simple transferencia electrónica.

- Difundir a PagoSeguro en Sitios de comercio electrónico, para que acepten establecer como una forma de pago, el proceso de PagoSeguro.

1.3 Alcances y limitaciones

1.3.1 Alcances del Sistema

Los alcances del Sistema son resultado de las fortalezas de sus procesos y funcionalidad, y se enumeran a continuación:

- El Sistema realiza un proceso de verificación del registro del usuario, para certificarse que quien se registra con un correo determinado, sea quien dice ser, por esto emplea el proceso de confirmación de la cuenta por correo.

- El registro de datos personales y financieros y sus correspondientes actualizaciones, se realizan a través de una conexión segura con PagoSeguro

- Los datos financieros (número de cuenta bancaria, número de tarjeta de crédito), son validados con la correspondiente Institución Financiera, para certificar la originalidad de los mismos.

- El proceso de recepción o envío de dinero, se realiza de manera segura, y sólo se acepta la transacción si el correo del destinatario está registrado en PagoSeguro.

- El sitio provee una interfaz gráfica de fácil uso que lo guía de manera comprensible en todos los procesos de transferencias, actualizaciones e historial, en PagoSeguro

- Se proporciona al usuario la facilidad de un historial de transacciones, para que pueda chequear todos sus movimientos en cualquier tiempo.

- El sistema por ser un sitio en línea, está desarrollado en tecnología web, con capacidades de portabilidad, por lo tanto puede ser accesado desde un cliente browser en cualquier parte del mundo con una computadora con acceso a Internet.

- Encriptación de la información personal y financiera de los usuarios de PagoSeguro.

1.3.2 Limitaciones del Sistema

- El sistema, en su inicio proveerá servicios sólo en Ecuador.

- La infraestructura tecnológica sobre la que esta montada el Sistema, deriva un mantenimiento y administración, que debe ser realizado sólo por parte de personal capacitado.

CAPÍTULO II

ANÁLISIS DE MERCADO DE UN SISTEMA DE PAGOS ELECTRÓNICOS

Uno de los principales obstáculos que ha tenido el desarrollo del comercio electrónico es la falta de confianza del usuario en Internet como un medio seguro de compra y pago de bienes y/o servicios.

Sin embargo, nadie puede demostrar que es más inseguro comprar en Internet que en cualquier otro sitio físico, ni que sea más fácil el robo de datos en las transacciones electrónicas que en los pagos con tarjeta de crédito en comercios o restaurantes, o al utilizar cajeros automáticos. Pero la proliferación de noticias sobre ‘hackers’, virus y fraude online ha contribuido a crear un clima poco propicio para que aumenten las cifras de compras por este medio.

Al comprar en Internet con tarjeta de crédito, tanto la validación como la realización efectiva del pago se realizan mediante el mismo sistema que se usa en un comercio convencional. Una vez que el número de tarjeta llega al vendedor, éste lo envía fuera de Internet de la misma forma que al pagar en cualquier tienda física. Por tanto, el punto crítico se produce al remitir el número de tarjeta a través de una red pública y potencialmente insegura como es el Internet.

Por eso, nuestro negocio en línea ofrece un medio alternativo de pago para ser utilizado en los sitios de comercio electrónico, de forma que el cliente final pueda tener la alternativa de utilizar tanto la tarjeta de crédito, como débitos directos a su cuenta bancaria preferida, con la diferencia de que sólo por una única ocasión ingresara la información sensible y privada en un formulario de Internet, y luego podrá realizar las compras que desee sin necesidad de dar esta misma información en todos los sitios de compras que visite.

El nombre de nuestro sitio es PagoSeguro.com

Este nombre afianza nuestra misión del negocio como tal, el de ofrecer un medio de pago Seguro para clientes y negocios de comercio electrónico.

2.1 Descripción de Servicios

Nuestros servicios son los siguientes:

2.1.1 Cuenta bancaria virtual gratis

Los clientes del sitio tendrán una Cuenta bancaria Virtual de forma gratuita, a la cual solo podrán acceder con su cuenta de correo y una contraseña debidamente autenticados y a través de un canal seguro de comunicación vía Internet.

2.1.2 Envío y recepción de dinero a cuentas de correo

Los clientes de PagoSeguro.com podrán enviar dinero a través de su cuenta de correo, a su vez indicando solo la cuenta de correo del beneficiario.

De la misma manera, podrán recibir dinero de otros clientes de PagoSeguro.com, directamente a su cuenta virtual y siempre recibirán notificaciones en su cuenta de correo.

2.1.3 Depósitos y retiros de dinero

Los clientes de PagoSeguro.com pueden agregar o retirar fondos de su cuenta virtual, con su correspondiente transacción a su tarjeta de crédito o cuenta bancaria.

2.1.4 Pago de servicios/bienes en sitios de comercio electrónico

Los clientes de PagoSeguro.com pueden realizar compras de bienes y/o servicios en los sitios de comercio electrónico afiliados a PagoSeguro.com, sin necesidad de dar su información confidencial de crédito a cualquier establecimiento.

PagoSeguro.com realizará las notificaciones necesarias para que la transacción comercial cumpla con los requisitos de ley.

2.1.5 Forma de pago para las empresas

Los clientes que sean empresas con negocios de comercio electrónico, podrán ofrecer en sus sitios web, el método de pago a través de PagoSeguro.com.

PagoSeguro.com proveerá de un botón mediante el cual el cliente final podrá escoger realizar el pago de su compra a través de las cuentas virtuales de PagoSeguro.com

2.2 Necesidad del Mercado

Un requisito indispensable para el desarrollo del comercio electrónico es contar con el marco legal adecuado.

Mediante Ley No. 67 se expidió La Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, aprobada por el H. Congreso Nacional del Ecuador el 17 de Abril del 2002 y su Reglamento; pero existen divergencias entre estos dos documentos lo cual hace difícil poner en práctica la ley.

Sin embargo, podemos decir que en nuestro país, cada vez estamos más cerca de promover de manera legal los negocios a través del Internet. Por lo tanto, la necesidad de formas de pago seguras a través de este medio se hace cada vez mayor.

En nuestro medio el uso de la tarjeta de crédito como forma de pago, siempre está dirigido a los establecimientos comerciales. Por razones más que todo culturales, la gran mayoría de los tarjeta habientes son escépticos ante las nuevas tecnologías de seguridad informática, que pueden garantizar el uso correcto de la información de la tarjeta de crédito a través de Internet.

A esto se suma los grandes casos de fraude conocidos mundialmente, de hackers que han violado las seguridades de empresas y corporaciones para el robo de información.

A su vez, las empresas cada vez más están convencidas que deben ofrecer valores agregados a sus productos o servicios sobre todo para fidelizar a sus clientes, ante la gran oferta de competencia del mercado. Y el Internet se convierte en una oportunidad de negocio, por no estar muy explorado y explotado en el país.

Pero ante esta gran oportunidad, hay riesgos. Primero, por que la ley de comercio electrónico no esta reglamentada correctamente y no permite una aplicación práctica de la misma, y segundo; sólo las grandes corporaciones financieras en su mayoría pueden acceder a los mecanismos de autenticación de las tarjetas de crédito internacional, lo que dificulta que una mediana o pequeña empresa pueda ofrecer un servicio de pago a través de Internet que garantice una transacción segura.

De todo esto, se pueden vislumbrar las siguientes necesidades orientadas a satisfacer la demanda del mercado actual:

- Los consumidores finales tienen la necesidad de contar con una forma de pago no exclusiva para acceder a los servicios o bienes ofrecidos por los negocios en Internet, la cual garantice una transacción segura y la integridad de la información privada proporcionada para ello.

- Las empresas del medio necesitan ofrecer sus servicios en Internet, de forma de captar un nuevo segmento de mercado, ofreciendo transacciones seguras de pago, no solo por los medios convencionales como tarjeta de crédito, sino también transacciones a cuentas bancarias de entidades financieras reconocidas del país.

- Medios alternativos de pagos en línea y envío de dinero ante el gran crecimiento de migrantes en el exterior, quienes en lugar de enviar remesas de manera convencional, pueden hacerlo de una manera más transparente y sin intermediarios y comisiones excesivas.

- Existen negocios que se pueden proveer en línea y que no justifican el uso de tarjeta de crédito como forma de pago, ya que no se compensa

por los costos bajos de comisiones. Esto se lo conoce como micropagos o pagos pequeños, como son suscripciones, descargas, donaciones, etc.

- Las empresas quieren convertir sus sitios web en negocios seguros, sin necesidad de desarrollar una solución tecnológica de seguridad propia, de forma de evitar los costos y responsabilidades de desarrollo que no son el núcleo de su propio negocio.

2.3 Análisis de la competencia

En nuestro país el comercio electrónico está empezando a tomar forma, por lo tanto no hay hasta el momento muchas compañías que ofrezcan el mismo servicio, es decir un sitio de pago seguro.
La mayoría de sitios online implementan formas de pago en alianza con una entidad financiera o emisora de tarjetas de crédito.

Si nos orientamos solo a la facilidad de enviar y recibir dinero, este es un negocio que está desarrollándose con los giros del exterior por la gran migración de los últimos años. Pero nuestro sitio no está por completo dirigido a este segmento de mercado aunque se proporciona esta alternativa dentro de sus servicios.

A nivel nacional, podemos mencionar los siguientes posibles competidores de nuestro sitio de pago:

e-pagos

www.todo1.com

Productos/Servicios

- Clientes Diners, Visa y Banco del Pichincha, pueden realizar compras en línea en los sitios de e-commerce que cuenten con este servicio.
- Negocios en línea pueden solicitar contar con este servicio de pago.

Formas de Pago

- Tarjetas de crédito Diners Club Internacional
- Tarjetas de Crédito Visa (Banco de Manabí, Banco de Machala, Mutualista Azuay, Banco Amazonas, Banco del Pichincha, Banco de Loja)
- Débito a las cuentas corrientes o ahorros del Banco del Pichincha.

Tarifas

- No tienen ningún costo para el Comprador.
- No se conoce el costo para el sitio Vendedor. Debe poseer cuenta bancaria en la institución.
- El Comprador debe poseer cuenta bancaria o tarjeta de crédito de la institución.

Seguridad

- Firma digital para la tienda virtual para encriptación de facturas y órdenes de pago.
- Uso de estándar de seguridad SSL para integridad de la información.

www.eprepago.com

e-prepago

Son tarjetas adquiridas para tener dinero prepagado para compras en Internet en los establecimientos autorizados.

Es un producto al parecer no comercializado aún.

Tarifas

No se conocen al momento

A nivel internacional, el sitio de pago más conocido es PayPal:

PayPal

Servicios

- Envíos y recepción de pagos a través de Internet.

Formas de pago

- Tarjetas de crédito Visa Internacional, Mastercard, Discovery y American Express

Seguridad

- El sitio de comercio electrónico no obtiene información sensitiva del comprador.
- Sistema de encriptación de datos de 128 bits, servidor seguro.
- Seguro gratuito por cada operación contra cualquier tipo de incidencia fraudulenta de $ 100.000.

Tarifas

- Es gratis para los compradores
- No se conoce un costo fijo para el negocio o vendedor.

2.4 Segmento de mercado

Nuestro sitio de pago es un enlace entre compradores y vendedores en línea. Es un medio seguro en el que se puedan fundamentar relaciones comerciales en ambos sentidos.

Por eso se considera que nuestro negocio estará dirigido a satisfacer las necesidades de dos grandes segmentos:

2.4.1 Compradores en línea.

Mercado natural de compradores de bienes y/o servicios que se ofrecen en línea, que incluyan la distribución o entrega del producto dentro del país.

Naturaleza del mercado: Natural.

Edad: De 25 a 45 años

Nacionalidad: Ecuatorianos o extranjeros

Clase económica: media a media alta

Medio de pago: tarjeta de crédito nacional, o tienen cuenta bancaria en instituciones financieras nacionales.

Descripción adicional: En su mayoría utilizan una computadora para su trabajo diario. Tienen acceso fácil a la navegación por Internet y estén familiarizados en la utilización de la tarjeta de crédito en sitios comercio electrónico o consultas de movimientos de cuentas bancarias.

Dentro de este grupo podemos también orientarnos a un segmento de mercado en gran crecimiento, que es la población migrante en el exterior, que constantemente realizan remesas de dinero a nuestro país.

2.4.2 Vendedores en línea

Mercado empresarial o de personas jurídicas, quienes tienen implementado un sitio en Internet para comercializar sus productos pero necesitan una forma de pago segura para ofrecer a sus clientes.

Naturaleza del mercado: Jurídico

Tamaño de la empresa: pequeña a mediana empresa

Nacionalidad: Ecuatorianos o extranjeros

Descripción adicional: Empresas o negocios que mantengan un sitio de comercio electrónico o deseen incursionar en este medio, ofreciendo una forma de pago de fácil acceso para el consumidor final y que no recurra a demasiados costos operativos o a grandes inversiones en tecnología de seguridad de información.

2.5 Estrategia de Mercado

Para poder establecer una estrategia de mercado de nuestro sitio PagoSeguro.com, se realizó un análisis DOFA de los servicios a ofrecer:

Debilidades

- El uso de tarjeta de crédito a través de Internet en nuestro país es una actividad muy poco usada, por lo tanto se tendrá muy pocos usuarios al inicio del proyecto.
- Existe ya un sitio que ofrece este servicio por medio de una Institución Financiera de gran aceptación en el mercado.

Oportunidades

- No hay en el mercado un sitio que ofrezca el servicio para cualquier usuario de tarjeta de crédito nacional.
- No hay en el mercado un sitio que ofrezca el servicio para usuarios que no posean tarjeta de crédito, sino cuenta bancaria.
- Existen Instituciones Financieras que no promueven todavía este tipo de servicios.
- A nivel nacional no existe un negocio de este tipo que ofrezca sus servicios para los migrantes ecuatorianos.

Fortalezas

- Ofrecer el servicio para clientes de tarjeta de crédito y clientes de cuenta bancaria.
- Seguridad en el manejo de la información sensible, registro por única vez.

- Servicios para uso de negocios nacionales.
- Sitio amigable al usuario, con opciones funcionales y prácticas.

Amenazas

- Puede surgir en cualquier momento un negocio parecido, por el creciente aumento de los negocios de comercio electrónico.

Después de realizar el análisis anterior, podemos indicar que nuestra estrategia de mercado será la siguiente:

- Establecer alianzas estratégicas comerciales con Entidades Financieras que deseen captar el mercado de negocios en línea, de manera de ofrecer los servicios de tarjeta de crédito y débito a cuenta bancaria en el sitio de pago.

- Revisar y levantar información de los negocios que ya estén en línea pero que ofrecen sitios solo con información estática y no incluyan servicios de comercio electrónico por falta capacidad tecnológica. Pequeña y mediana empresa.

- Realizar un lanzamiento del sitio para realizar donaciones a algún acto benéfico, de manera de dar a conocer la funcionalidad del servicio entre clientes y posibles sitios de comercio electrónico.

- Ofrecer el servicio a empresas que ofrecen servicios de afiliaciones o suscripciones de sus clientes. El estar en Internet es una ventaja competitiva ante el resto de ofertas en el mercado.

2.6 Justificación del negocio

Una vez demostrada la oportunidad de negocio en el mercado nacional para un sistema de pago electrónico, procedemos a indicar la justificación económica de la rentabilidad del proyecto

El principal costo operativo presente son las comunicaciones, ya que por la naturaleza del negocio debemos estar siempre en constante comunicación con las entidades financieras para las validaciones de los respectivos datos financieros de los clientes. Para ello la opción mas viable es buscar una entidad que ya disponga de una infraestructura de comunicaciones con enlaces a las diferentes instituciones financieras y con la posibilidad de procesamiento de tarjetas de crédito. Estas entidades son las llamadas procesadoras de tarjetas de crédito las cuales tienen comunicación con los

bancos y con los organismos de emisores de tarjetas de crédito internacionales como lo son Mastercard y Visa.

Para poder reducir el monto de la inversión inicial, así como los costos operativos mensuales correspondientes a comunicaciones, se propone establecer contratos comerciales con las Procesadoras de Tarjetas de Crédito, para poder usar los servicios de verificación y autorizaciones que estas ya ejecutan a través de sus infraestructuras de operación y comunicación que ya tienen implementadas.

De forma tal que a PagoSeguro le correspondería únicamente cancelar el servicio prestado por verificación y autorización de cada transacción procesada.

El costo para Pagoseguro puede ser por transacción verificada, o mejor aun por volumen de transacciones, modalidad con la que actualmente trabajan con ciertos establecimientos comerciales.

En el caso de la verificación de información de cuentas bancarias, a su vez se puede recurrir a un acuerdo comercial con Banred, quien es la entidad que opera con todas las entidades financieras en la verificación de transacciones en los cajeros automáticos.

De esta manera se puede disponer de este recurso, sin necesidad de tener enlaces de comunicación establecidos con las diferentes entidades financieras, recurriendo solo en costos por utilización del servicio de verificación y aceptación de transacciones

Para el depósito en cuentas físicas del dinero de clientes de Pagoseguro se tiene la opción de usar el sistema de Grandes pagos (SPI) del Banco Central del Ecuador, que opera con todas las entidades financieras a nivel nacional para efectuar transferencias interbancarias.

Definido este esquema de trabajo cooperativo, solo se tendría que establecer canales de comunicación directos y seguros a la Procesadora con la cual se establezca el acuerdo así como, el enlace de comunicación con Banred y la creación de la cuenta en el BCE para utilizar el SPI, esta interconexión y operación está representada en la figura adjunta al apéndice

Ingresos

Se definen las siguientes tarifas por los servicios ofrecidos en PagoSeguro:

TIPO DE TRANSACCIÓN PAGOSEGURO	COSTO DEL SERVICIO
Registro de Cuenta	$ 0.00
Ingreso de Saldo	1% sobre el monto a Ingresar
Envío de dinero	$ 0.00
Pago en línea a comercio asociado	Para el comprador es sin costo. Para el vendedor (comercio asociado), el costo es de $ 1.50 por cada pago.
Retiro de fondos	$ 1 por cada retiro, sin importar el monto del mismo.

Tabla 1 Costos de transacciones en pagoseguro

- El monto mínimo de Depósito o Ingreso a la cuenta virtual es de $ 50.00

Egresos

Se ha realizado una investigación de los costos de los servicios de verificación y confirmación de transacciones entre operadoras de tarjetas de crédito y cuentas bancarias, de lo cual podemos estimar que los siguientes valores son los que se cancelarían por estos servicios a la Procesadora de Tarjetas de Crédito y arred, aliados comerciales propuestos para la implementación del negocio:

TRANSACCIÓN CON TARJETA DE CRÉDITO	VOLUMEN DE TRANSACCIONES AL MES	COSTO POR TRANSACCIÓN
Verificación de tarjeta de crédito	1- 50	$ 0.25
Verificación de tarjeta de crédito	50 en adelante	$ 0.18
Avance de Efectivo	1- 50	$ 0.30
Avance de Efectivo	50 en adelante	$ 0.15
Autorización (pago online)	1 – 50	$ 0.20
Autorización (pago online)	50 en adelante	$ 0.12

Tabla 2 Estimación de transacciones de tarjetas de crédito

TRANSACCIÓN CON CUENTA BANCARIA	COSTO POR TRANSACCIÓN
Verificación de cuenta bancaria	$ 0.35
Transferencia entre cuentas	$ 0.40

Tabla 3 Estimación de transacciones de cuentas

Correspondencia de transacciones

TRANSACCIÓN PAGO SEGURO	TIPO	PROCESADORA DE TARJETA	BANRED
Ingreso de Saldo primera vez	Tarjeta de crédito	Verificación Avance de Efectivo	
Ingreso de Saldo	Tarjeta de crédito	Avance de Efectivo	
Retiro de fondos	Tarjeta de crédito		Transferencia de cuenta *
Pago electrónico	Tarjeta de crédito	Autorización	
Ingreso de Saldo primera	Cuenta bancaria		Verificación Transferencia

vez			de cuenta
Ingreso de Saldo	Cuenta bancaria		Transferencia de cuenta
Retiro de fondos	Cuenta bancaria		Transferencia de cuenta
Pago electrónico	Cuenta bancaria		Transferencia de cuenta

- Se considera que las transferencias son entre cuentas de una misma entidad financiera.

Tabla 4 Correspondencia de transaaciones

Inversión Inicial

Cantidad	Item	Valor
HARDWARE		
	Centro de cómputo	
1	Servidor de Base de Datos	$ 6,000.00
1	Servidor de Base de Datos de Contingencia	$ 6,000.00
1	Servidor de Aplicaciones y Web	$ 5,000.00
1	Servidor Firewall Base de Datos – Web	$ 5,000.00
1	Servidor Firewall interno	$ 5,000.00
1	Router (Internet)	$ 1,800.00
1	Switch capa 3	$ 1,600.00
1	Arreglo de discos	$ 3,000.00
	Administración	
3	Computadores de escritorio	$ 3,000.00
1	Impresora multifunción	$ 500.00
		$ 36,900.00
SOFTWARE		
15	Licencias de Oracle Standard Database 10g	$ 4,500.00
3	Licencias de Windows 2000 Pro	$ 600.00
		$ 5,100.00

INSTALACIONES		
	Mobiliario	$ 2,000.00
	Instalación de enlaces de comunicación	$ 700.00
		$ 2,700.00
TOTAL INVERSIÓN INICIAL		**$ 44,700.00**

Tabla 5 Rubros de inversión inicial

Ingresos mensuales

Fortaleciendo las estrategias de mercado, se espera llegar a los siguientes volúmenes de transacciones mensuales:

SERVICIOS	TRANSACCIONES	INGRESOS
Ingreso de saldo (1era vez)	200 *	$ 100.00
Ingreso de saldos	4000 **	$ 4,000.00
Pagos online	4000	$ 6,000.00
Retiros de fondos	200	$ 200.00
TOTAL INGRESOS		**$ 10,300.00**

*Se ha considerado que por primera vez se ingresa el saldo mínimo de $ 50.00
**Se ha considerado que los montos en promedio son de $ 100.00

Tabla 6 Estimado de ingresos en pagoseguro

Costos y Gastos mensuales

COSTOS Y GASTOS	VALOR
Costos Operativos Fijos	
Ultima milla Internet	$ 800.00
Enlace FR 128K Procesadora	$ 300.00
Enlace FR 128K Banred	$ 300.00
Nómina	$ 2,000.00
	$ 3,400.00
Costos Operativos Variables	

Servicios de verificación de información Procesador	$ 800.00
Servicios de verificación de información Banred	$ 1,000.00
Servicios básicos	$ 250.00
Arriendo	$ 200.00
Suministros de oficina	$ 30.00
Suministros de cómputo	$ 60.00
Mantenimiento de equipos	$ 45.00
	$ 2,385.00
TOTAL COSTOS Y GASTOS	**$ 5,785.00**
UTILIDAD MENSUAL	**$ 4,515.00**
RENTABILIDAD MENSUAL	**43.83 %**
INGRESOS ANUALES	**$ 123,600.00**
INVERSION INICIAL	**$ 44,700.00**
ROI (Tasa Retorno de la Inversión)	**21 %**
	12 meses

Tabla 7 Rubros de egresos y utilidad en pagoseguro

CAPÍTULO III

ANÁLISIS Y DISEÑO DE UNA INFRAESTRUCTURA DE RED SEGURA PARA EL SITIO DEL SISTEMA DE PAGO ELECTRÓNICO

3.1 Selección de mecanismos de seguridad

En la actualidad, existen varios mecanismos de seguridad que pueden ser implementados en una organización o en una solución de negocios electrónicos, como un sistema de pagos electrónicos en línea.

Cada uno de estos mecanismos siempre cumplirá con su objetivo de disminuir los riesgos de un ataque o intrusión a la información vital para el negocio. Es decir, que siempre proveerán servicios y soporte a la seguridad de la información. [STAL]

Para el efecto, se ha subdivido a estos mecanismos en dos categorías:

- Mecanismos de seguridad específicos, y
- Mecanismos de seguridad penetrantes

A continuación detallaremos el significado de cada uno de las categorías de los mecanismos de seguridad.

3.1.1. Mecanismos de seguridad específicos

Esta categoría son todos aquellos mecanismos usados para proveer la seguridad a servicios específicos.

En base a esta definición, esta categoría se divide en ocho tipos de mecanismos de servicios específicos, los cuales son:

- Cifrado
- Firmas digitales
- Control de acceso
- Integridad de datos
- Autenticación
- Control de ruteo
- Notarización

3.1.1.1 Cifrado

El cifrado es una de las principales técnicas de mecanismos de seguridad en la actualidad, siguiendo los objetivos principales de la criptografía en cuanto a seguridad de la información se refiere, los cuales son: confidencialidad, integridad, autenticación y no repudio. El cifrado viene desarrollándose desde hace muchos años atrás, incluso desde la época de los egipcios, con un lenguaje limitado pero que dio el inicio a los mensajes cifrados.

Con el pasar de los años se han ido realizando mejoras con respecto a estas técnicas matemáticas, se han creado nuevos algoritmos, nuevos esquemas de cifrado, para cada uno de ellos ha considerado criterios tales como, el

nivel de seguridad, la funcionalidad, métodos de operación, rendimiento, y la facilidad de implementación.

El cifrado ha sido de importante uso en las áreas de comunicaciones militares, gubernamentales principalmente ya que por la privacidad de los mensajes y la autenticidad de las mismas, se requería completa confidencialidad y de evitar intersecciones de los mensajes, por eso era necesario codificarlos, y verificar su validez. A fin de cumplir estas necesidades, se fueron creando nuevos esquemas de cifrado, esquemas de clave pública y privada, firmas digitales. Hoy en día estos esquemas son perfeccionados y han llegado al punto de ser casi indescifrables, y el uso es ahora muy amplio, como en comunicaciones electrónicas, correos electrónicos, transacciones bancarias electrónicas y demás.

Los esquemas de encriptación y desencriptación que existen, son sencillamente transformaciones que sufren diferentes funciones matemáticas a fin de obtener un resultado complejo, a este proceso también se lo conoce como cifrado. Otro de los esquemas existentes es del de la encriptación de clave simétrica, del cual se deriva cifrado por bloques, en el que el mensaje a ser cifrado, se consideran bloques limitado de datos, es decir de igual tamaño, para ser procesados computacionalmente y lograr cifrar su contenido, es decir lograr una transformación del mensaje original,

para luego, ser descifrado mediante la clave con la que el tamaño del bloque fue definido inicialmente, es decir volver a procesar la información pero de manera inversa. Para este esquema de cifrado de bloques, se divide en dos clases: el cifrado de sustitución y el de transposición.

Cifrado de simple sustitución

Esta transformación consiste en permutar cada elemento del mensaje para luego ser sustituidos con cada elemento de la permutación.

Cifrado de transposición

Esta sólo consiste en permutar los símbolos en un bloque, por tal motivo es fácilmente criptoanalizado. Es decir que es fácilmente descifrable.

El otro esquema de cifrado mediante claves simétricas, es el cifrado de flujo, el cual consiste en el cifrado de bloques pero con un tamaño fijo de uno para cada bloque. La principal ventaja de este, es que la tasa de error durante la propagación, disminuye.

3.1.1.2 Firmas digitales

Las firmas digitales son creadas y verificadas por la criptografía, esta es una rama de las matemáticas que hace posible la transformación de los mensajes a una forma ilegible. El uso de las firmas digitales es conocida también como

“criptografía de clave pública”, en el que se emplea algoritmos matemáticos para generar y usar dos claves relacionados matemáticamente, una se utiliza para crear la transformación de los datos en forma ilegible y la otra se usa para verificar los datos y transformar los datos al mensaje original.

En la actualidad existe software y equipos informáticos que utilizan un esquema de criptografía asimétrica. Los sistemas de criptografía asimétrica para firmas digitales se usan términos como clave privada, el cual es solamente conocida por quien firma, es decir que es usada para generar la firma digital. Mientras que el término, clave pública, la cual es conocida ampliamente y usada por las partes involucradas en verificar la autenticidad de la firma digital. Por tanto, cuando la información que se transmite usando firmas digitales, es necesario conocer y tener acceso a un repositorio de claves públicas para poder verificar y descifrar la información recibida firmada digitalmente. Si este sistema de criptografía asimétrica ha sido diseñado e implementado de manera segura, por tanto será un sistema casi infalible.

Las funciones hash, son otros de los procesos fundamentales para la creación y verificación de las firmas digitales. Una función hash es un algoritmo que crea una representación digital o “fingerprint” en la forma de un valor hash o resultado hash de una longitud estándar, el cual es mucho más pequeño que el mensaje pero esencialmente es único.

Cuando se usa funciones hash seguras, los mensajes son casi infalibles.

El uso de firma digitales involucra dos procesos, uno para el que genera la firma y el otro para el receptor de la firma digital.

- Creación de la firma digital, usa un resultado de la función hash único del mensaje firmado y de la clave privada proporcionada. Para que esta sea segura, debe haber solamente una posibilidad insignificante que la misma firma digital se podría crear por la combinación de cualquier otro mensaje o llave privada.
- Verificación de la firma digital, este es el proceso de verificación de la firma digital, con referencia al mensaje original y a la clave pública proporcionada, determinando si la firma digital fue creada usando el mensaje y la clave privada correspondiente.

Típicamente, una firma digital (un resultado de la función hash del mensaje) se une a su mensaje y se almacena o se transmite con su mensaje. Sin embargo, puede también ser enviada o ser almacenada como elemento de datos separado, siempre y cuando mantenga una asociación confiable con su mensaje. Puesto que una firma digital es única a su mensaje, es inútil si se separa enteramente de su mensaje.

Varios sistemas de criptografía asimétrica crean y verifican las firmas digitales usando diferentes algoritmos y procedimientos, pero sobre todo comparten los mismos patrones operacionales, tales como:

- Autenticación del firmante, si el par de claves privada y pública son asociadas con un firmante identificado, la firma digital atribuye el mensaje del firmante identificado, por lo tanto, esta firma digital debe ser almacenada en lugar seguro y no debe extraviarse ni divulgarse.
- Autenticación del mensaje, la firma digital también identifica al mensaje firmado, la verificación revela cualquier forzamiento, puesto que la comparación de los resultados de la función hash (uno hecho en la firma y el otro hecho al verificar) demuestra si el mensaje es igual que cuando estaba firmado.
- Acto afirmativo, crear una firma digital requiere a un firmante a utilizar la llave privada del firmante. Este acto puede realizar la función "ceremonial" de alertar al firmante el hecho de que el firmante está llevando una transacción a cabo con consecuencias legales.
- Eficiencia, los procesos de crear y de verificar una firma digital proporcionan un alto nivel del aseguramiento que la firma digital sea genuino del firmante. Como con el caso de datos electrónicos modernos de intercambio ("EDI") la creación y los procesos de la verificación son capaces de la automatización completa (designada a veces

"machinable"), con la interacción humana requerida solo con excepciones. Comparado a los métodos de papel tales como comprobación de las tarjetas de la firma de espécimen -- métodos tan aburridos y dependientes de trabajo que se utilizan raramente realmente en la práctica -- producción digital de las firmas que un alto grado de aseguramiento sin la adición grandemente a los recursos requeridos para procesar.

Las firmas digitales se han aceptado en varios estándares nacionales e internacionales desarrollados en la cooperación con muchas corporaciones, bancos, y agencias de estatal que las han aceptado.

3.1.1.3 Control de acceso

Se define como los mecanismos necesarios para determinar el acceso a objetos o dispositivos en la red para ser administrados. Además del control de acceso se deben definir políticas de acceso a los dispositivos

Para lograr esta definición se puede utilizar el siguiente gráfico (Figura 1) para ilustrar el concepto de este mecanismo de control de accesos.

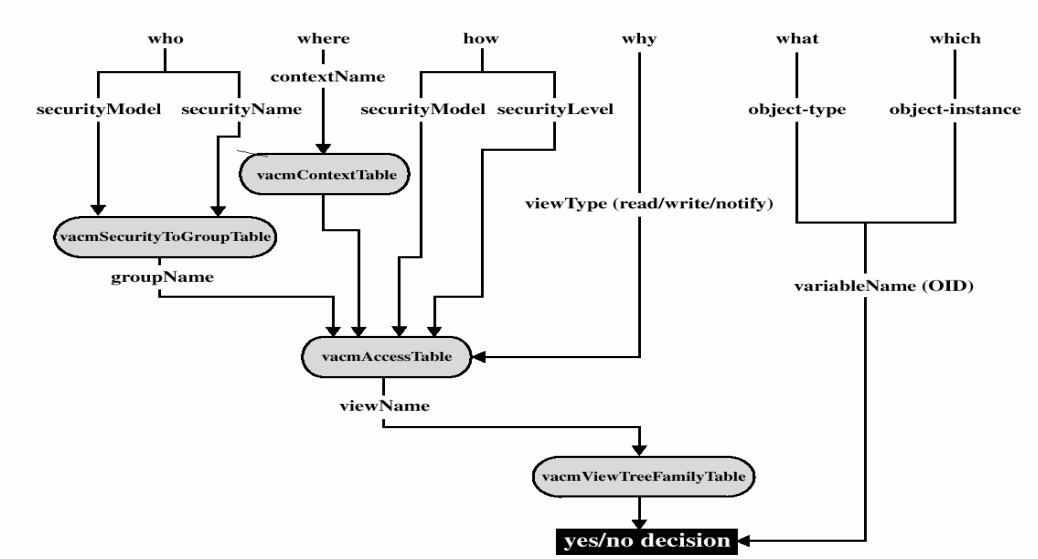


Figura 1 Ejemplo de esquema de control de acceso

Por lo tanto, es necesario e importante identificar cada uno de los agentes que tendrán acceso a los diferentes objetos, dispositivos y elementos activos del sistema de información y también considerar el acceso a la infraestructura de la red que soporta el flujo de información.

Estos mecanismos de control de acceso aplica tanto a dispositivos de hardware como servidores, switches, firewalls, u otro elemento como parte activa de la red, así como también controlar el acceso de usuarios hacia los datos que se almacenan en un repositorio, o durante el flujo de la información entre dispositivos. Para esto a nivel de software sobre los sistemas de información se define lo que se conoce como listas de control de acceso, que son una serie de reglas ordenadas con cierta prioridad para permitir o negar el acceso a un objeto del sistema en general.

Esto también evitará el acceso a usuarios remotos, la ejecución de código malicioso en los servidores y aplicaciones, etc.

Otro de la formas de definir el control de acceso, es definiendo las capacidades que tiene cada agente, o también definir niveles de seguridad.

Para nuestro sitio, se ha considerado cada uno estos criterios para escoger los más importantes que deberían ser aplicados sobre nuestra infraestructura de red y el software a utilizar.

3.1.1.4 Integridad de datos

En todo sistema de información y principalmente en el diseño de la infraestructura de un sitio de comercio electrónico, lo más importante es la consistencia de los datos, es decir, la confidencialidad e integridad de los mismos, ya que son la esencia o base del negocio. Por tanto, se requiere que existan mecanismos que aseguren la integridad de los datos desde el inicio hasta el final del negocio. Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

Técnicas como el respaldo de datos, balanceo de carga de datos, son algunas de las formas de mantener los datos íntegros y disponibles en el tiempo que se mantenga en línea el negocio.

3.1.1.5 Autenticación

Este mecanismo consiste en corroborar que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

Actualmente existen protocolos que permiten mantener un canal seguro durante la autenticación, tal es el protocolo LDAP (Lightweight Directory Access Protocol), el cual consiste en un servicio que mantiene un repositorio de información de usuarios, y el proceso de autenticación se realiza contra un servidor que provea el servicio habilitando un canal seguro para esta transmisión de datos. A fin de evitar que sea olfateada, el usuario y contraseña, e incluso sea interferida por agentes extraños en una red. Esto es usando el protocolo LDAPS, es decir, que se abre una conexión segura contra el protocolo LDAP.

3.1.1.6 Control de ruteo

El control de ruteo, permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

3.1.1.7 Tráfico de relleno

Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

3.1.1.8 Unicidad

Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

3.1.2. Mecanismos de seguridad penetrantes

Esta categoría son todos aquellos mecanismos en los cuales no se especifican servicios particulares.

Se identifican principalmente cinco tipos:

Funcionalidad confiable

Cualquier mecanismo de seguridad que se provea siempre debe prestar la mayor confiabilidad posible.

Se puede realizar una combinación de software y hardware para alcanzar esta confiabilidad.

Etiqueta de seguridad

Cualquier recurso tales como; datos, comunicaciones de banda ancha pueden tener un etiqueta de la seguridad asociada a él para indicar sensibilidad de la seguridad.

Las etiquetas se pueden asociar semejantemente a los usuarios. Las etiquetas pueden necesitar estar limitado con seguridad a los datos transferidos.

Detección de eventos

La detección de eventos incluye características como, intento de violaciones de seguridad y actividades legítimas relacionadas a la seguridad.

Entran en juego sistemas como, detección de intrusos, logging o monitoreo, tales sistemas permiten la detección y evasión de intrusos a la infraestructura de la red.

Seguimiento de rastros de seguridad

Con este mecanismo se debe mantener un registro de los últimos acontecimientos relacionados a seguridad, además de permitir la detección e investigación en el posible caso de un ataque a la red.

Recuperación de la seguridad

Establecer planes de contingencia, o mecanismos que permitan la fácil recuperación de la seguridad cuando existan fallas o huecos en cada parte de la solución de negocios, es decir en cada elemento de la infraestructura de la red, del software y hardware.

Para este proyecto, se han considerado cada uno de estos mecanismos a fin de obtener los objetivos planteados en un esquema de alta disponibilidad y de seguridad. La mayoría de ellos son utilizados como herramientas de seguridad para la implementación de dicho proyecto, usando software o hardware que permitan la funcionalidad adecuada en cuanto a seguridad de la información se refiere. [STAL]

3.2 Selección de herramientas de seguridad

Para la selección de las herramientas de seguridad, nos hemos basado en todos los mecanismos de seguridad existentes, que pueden ser escogidos para la implementación casi segura de la infraestructura de la red y proteger así la información.

La decisión de escoger la mejor opción, es decir las mejores herramientas de seguridad, dependen principalmente de un presupuesto económicamente hablando, de que tanto se desea invertir para proteger todo los elementos

que constituyen la idea del negocio, es decir el sistema de pagos electrónicos en línea.

En el mercado nacional e internacional existen herramientas gratuitas, mas conocidas como open source; y aquellas que tienen un costo como las versiones comerciales, que se venden tradicionalmente como un paquete de software, para ello es necesario realizar exhaustivos análisis antes de comprar o decidirse por la opción gratuita. [ANOM]

Generalmente los principales criterios a considerar son: el soporte que brindan sobre la herramienta, costo, facilidad de administración, compatibilidad, requerimientos mínimos, garantía, entre otros.

Para nuestra infraestructura, nos hemos decidido por las aplicaciones de software económicas, de bajo costo, como es el open source.

Entre las principales razones que se consideraron para tal decisión, esta que el soporte aunque no es certificado, se puede conseguir muy fácilmente en algunos casos en la red de redes, como es la Internet. Además, estas herramientas se pueden ajustar fácilmente a nuestros requerimientos ya que se puede modificar el código, según la licencia de código abierto.

A diferencia de los productos comerciales que difícilmente o casi imposible nos es permitido cambiar el código para ajustarlos a nuestros requerimientos.

También pesa en nuestra decisión el saber que por ser un código abierto, no es sometido a bombardear huecos o fallas de seguridad en la programación del mismo, a diferencia de las versiones comerciales, en las que los hackers o intrusos dedican la mayor parte de su trabajo en estos, porque causan mucho daño a quienes lo adquirieron. Quizás unos de los factores que se sume como desventaja por este tipo de decisión, es durante la programación del sitio web, o de la aplicación, ya que el personal con conocimientos en el desarrollo y uso de estas herramientas gratuitas suele ser escaso, a diferencia de los productos comerciales, donde sí existe mucho personal capacitado y certificado para la programación de las diferentes aplicaciones.

El hardware que se pueda utilizar como herramienta de seguridad, digamos un firewall, ya no es una herramienta gratuita a nivel de hardware, una alternativa a esto es el software que realiza la misma función que un firewall, así también puede ser gratuito como también comercial.

En conclusión, en nuestra infraestructura de red y de solución de información, se puede llegar a tener ambas tecnologías, es decir gratuitas y comerciales, a fin de lograr la robustez necesaria para proteger nuestra idea de negocios. Lograremos una plataforma híbrida, como se conoce comúnmente.

Entre las principales herramientas tenemos: firewalls, sistemas de detección de intrusos (IDS), monitoreo (logging), antivirus, búsqueda de vulnerabilidades, sniffers.

Muchas de estas herramientas son consideradas muy importantes durante el funcionamiento de la solución informática, a fin de evitar las fortuitas intrusiones no autorizadas.

A continuación realizaremos el respectivo análisis de las herramientas seleccionadas.

3.2.1 Firewall

Es cualquier dispositivo usado como un mecanismo de control de acceso para proteger redes o múltiples redes del acceso no autorizado de intrusos. En un sentido más general, un firewall consiste de software y hardware. El software puede ser propietario, de demostración o gratuito. El hardware puede ser cualquier dispositivo que soporte el software. Son principalmente usados para crear puertos seguros para aplicaciones tales como, procesos de pagos electrónicos, sitios web seguros de transacciones bancarias, sitios de e-commerce, etc.

No son limitados a ser usados exclusivamente en el perímetro. Generalmente los firewalls son computadores, routers, o dispositivos específicamente que hacen la función de firewall. Es decir que es un hardware especializado para

realizar la tarea de control de acceso. Por ejemplo, el CISCO PIX series es un firewall de hardware.

Los firewalls son diseñados para servir como un punto de control en la red, siempre evalúan los requerimientos de conexiones que son recibidas. Estos, analizan el tráfico que puede ser permitido o no, basado en un grupo de reglas. Son solo procesados aquellos requerimientos de conexión autorizados, caso contrario son rechazados.

Muchos de los firewalls logran esto protegiendo el direccionamiento de origen y destino a lo largo de los números de los puertos.

Los firewalls pueden analizar paquetes entrantes y salientes de varios protocolos de red. Basándose en el análisis, un firewall puede decidir qué hacer con el paquete, es decir, tienen la capacidad de evaluar las condiciones.

Son las reglas o políticas las que hacen posible estas condiciones de análisis.

Hoy en día los firewalls tienen incorporadas nuevas funcionalidades, haciendo de ellos más eficientes y robustos.

Algunas de estas características son: filtrado de contenido, redes virtuales privadas (VPN), traducción de dirección de redes (NAT), balanceo de carga, tolerancia a fallos, detección de intrusos.

Las tecnologías de firewall son clasificadas en tres categorías:

- Packet filter-based
- Stateful packet filter-based
- Proxy –based

3.2.1.1 Packet filter

Son típicamente los routers, que tienen capacidades de filtrado de paquetes.

Con esto se puede otorgar o negar el acceso a un sitio basado en las siguientes variables:

- Dirección origen
- Dirección destino
- Protocolo
- Número de puerto

Este tipo de firewall es muy popular debido a su fácil implementación.

Sin embargo, tienen deficiencias. Usualmente no están preparados para manejar ciertos tipos de ataques como; DoS, denial of service. También el manejo de SYN flooding, o inundación de puertos, y otras anomalías basadas sobre el protocolo TCP/IP.

Otra de las deficiencias, es que no fueron diseñados para mantener pistas de los estados de las sesiones de datos establecidas. Por tal motivo los administradores son forzados a mantener todos los puertos sobre el 1024 a mantenerlos abiertos para manejo de sesiones y negociaciones

apropiadamente. No es una buena práctica mantener puertos abiertos sin usar, hacia la Internet.

Y finalmente, el uso de ACL, listas de control de acceso, contribuye a la degradación del rendimiento del hardware, es decir, índices altos de consumo de CPU, sobrecarga, lo que conlleva a conexiones más lentas.

3.2.1.2 Stateful packet filter

Este tipo de firewalls están construidos sobre la base del modelo de packet filter, pero con la característica adicional de mantener el rastro de las sesiones y conexiones en tablas de estados internas.

Estos firewalls pueden detectar situaciones anormales que intentan violar los protocolos standar. Por lo tanto, se bloquearán los ataques. Esto los hace más flexibles con respecto a los otros tipos de firewalls, además que protegen también de los tipos de ataques de DoS y servicios de correo en base a protocolo SMTP.

3.2.1.3 Proxy based

También conocido como application gateway o application Proxy. Consiste en que cuando un usuario remoto se contacta con una red protegida por un firewall Proxy, este se apodera de la conexión. Con esta técnica, los paquetes IP no son reenviados directamente hacia la red, en vez de eso,

ocurre un tipo de traslación, con lo que el firewall actúa como conductor e intérprete.

La diferencia de los demás firewalls, se basa en que este inspecciona el tráfico a nivel de la capa de aplicación y además los niveles más bajos. Un paquete entra al firewall proxy, y es dado a una aplicación específica del Proxy, el cual inspecciona la validez del paquete y el requerimiento por sí mismo.

Este concepto de acercamiento de protocolo a protocolo, es más seguro que los demás firewalls, porque el firewall entiende de los protocolos de aplicación por sí mismo, de lo contrario será rechazado aquello que no sea especificado. Esto dificulta a los instrusos de un posible ataque a través de puertos y direcciones.

3.2.2 Sistemas de detección de intrusos

Las palabras, *detección de intrusos,* significan muchas cosas a muchas personas; nosotros definiremos como el acto de detectar a un usuario hostil o intruso quién está intentando obtener acceso no autorizado. Basados en esta definición, un número de métodos populares son usados como detector de intrusos, tales como, sistemas de inspección, firewall, logs de ruteadores.

Las raíces de los sistemas de detección de intrusos o IDS de hoy en día, residen sobre los modelos de sistemas de detección de intrusos expertos (IDES) y de los sistemas de detección de intrusos distribuidos (DIDS), desarrollados por el departamento de defensa de los Estados Unidos desde los años 80 y 90. Sin embargo, los nuevos IDS, mantienen el mismo objetivo que sus predecesores, ayudar a automatizar el proceso de búsqueda de intrusos.

Actualmente a los IDS se los clasifica en las siguientes tres categorías:

- IDS de redes
- IDS de host
- IDS de anomalías

3.2.2.1 IDS basados en redes

Los sistemas de detección de intrusos basados en redes, llamados (NIDS) por sus siglas en inglés, consisten en capturar el tráfico de la red y

compararlo con un grupo de patrones o firmas de ataques conocidos. Estos comparan las firmas con cada paquete simple que ellos ven, en espera de atrapar un intruso en el acto. Este tipo de IDS puede ser desarrollado pasivamente, sin necesidad de requerir modificaciones sobre las redes.

3.2.2.2 IDS basados en host

Estos sistemas varían de un proveedor a otro, pero se concentran en el análisis. Este tipo de IDS tienen componentes que analizan el sistema, el login del usuario y los procesos.

Algunos de estos sistemas tienen capacidades para descubrir código troyano. Estos sistemas son basados en agentes, es decir que requieren la instalación de un programa sobre los sistemas que protege, esto permite un mayor nivel de protección pero mayor administración.

3.2.2.3 IDS basados en anomalías

Estos sistemas son un poco confusos y muchas veces son referidos como un concepto que un modelo actual. La filosofía detrás de los IDS basados en anomalías, es entender los patrones de los usuarios y tráfico sobre la red y encontrar las desviaciones en estos patrones.

Los IDS más comunes son los NIDS y HIDS, son los mas desarrollados y comerciales.

3.2.3 Criterios comunes de evaluación para escoger un IDS

Cuando se desea escoger un IDS, se debe escoger dos cosas, el producto y el proveedor. El proveedor es muy importante, ya que este permitirá obtener las actualizaciones del producto, de esta manera se podrá mantener al día las posibles fallas y huecos de seguridad que se encuentren en el producto. Un buen IDS llegará a mejorar con el paso del tiempo, incrementará su funcionalidad y por tanto se requiere de estas actualizaciones.

Para escoger el mejor IDS, o al menos el que mejor se ajuste a las necesidades de nuestra infraestructura de red, se deben considerar cada uno de los siguientes componentes principales, que deben existir en cualquier producto que realice la funcionalidad de un IDS, los cuales nos ayudarán a tomar una mejor decisión.

3.2.3.1 Profundidad de la cobertura

Este componente es muy importante, ya que el sistema debe tener la capacidad de detectar una amplia gama de ataques. Permitir la personalización de configuraciones, una administración diestra de las interfaces. Verificar que el producto permita el manejo de rastreo de ataques,

inspección de archivos de log a nivel de IDS basados en red y en hosts, además que soporte todas las plataformas que sean necesarias monitorear.

3.2.3.2 Exactitud de la cobertura

Este componente es un factor fuerte para determinar, sin pruebas minuciosas, que debería ser notado que no todas las firmas hayan sido creadas por igual.

Los falsos positivos son un gran problema con muchas soluciones de IDS basadas en redes, y en entornos grandes, este tipo de sucesos puede arriesgar la efectividad del esfuerzo realizado por el IDS.

Aquellos productos diseñados con reducción de falsos positivos, son más deseables.

3.2.3.3 Arquitectura robusta

En cada uno de los componentes del IDS, es importante que el núcleo y el framework de estos productos hayan sido diseñados con grandes fortalezas de seguridad.

Del lado del agente, debería ser capaz de resistir ataques y técnicas básicas de evasión. Aunque la evasión ha sido tradicionalmente un problema que ha plagado los dispositivos de IDS basados en redes, los proveedores de IDS han dirigido su atención a este tipo de problemas con gran esfuerzo. Algunos

han ignorado esto, con la cual han reducido la eficiencia del producto, por lo tanto han reducido la confianza de los profesionales de seguridad.

3.2.3.4 Escalabilidad

Entres los principales componentes en la escalabilidad de un sistema IDS que se ven afectados, son el monitoreo de redes de grandes anchos de banda y la administración de grandes volúmenes de datos. Algunos productos tienen serios problemas al realizar monitoreo a los dispositivos de grandes anchos de banda y entornos de gran volumen de sesiones. Así mismo, se presentan problemas en entornos con grandes volúmenes de datos, como almacenamiento. Algunos de estos problemas serían, la pérdida de los datos, sobrecargas, y además un incremento fuerte para el ordenamiento de las alertas de seguridad.

3.2.3.5 Administración de infraestructura

Así mismo como es importante la detección de intrusos, es también importante la capacidad de presentar claramente y eficientemente los datos sobre los ataques relacionados. Si esto no fuera posible, entonces el uso del IDS sería muy limitado. Por tanto, se debe considerar una consola de administración donde se puede observar cada uno de los eventos de acuerdo a la infraestructura implantada. Permitiendo la facilidad de acceso a esta

información por los agentes estrictamente necesarios, como son los administradores de seguridad.

3.2.3.6 Actualizaciones oportunas

Debido a la propagación rápida que suelen darse por la creación de un nuevo virus, o alguna nueva vulnerabilidad encontrada en algún sistema de IDS, es muy importante mantener la actualizaciones oportunas durante el tiempo de funcionamiento del mismo sobre las vulnerabilidades críticas y las actualizaciones del núcleo del IDS. Por ello, este componente es un factor muy considerable en la toma de decisión por un IDS.

3.2.3.7 Personalización

Algunos sistemas de detección de intrusos permiten un rango determinado de configuraciones, es decir, son muy estáticos e inflexibles. Para ciertos entornos no es necesaria esta característica, porque se ajustan a sus necesidades, pero en otros entornos sí es necesario tener acceso a una gran gama de configuraciones del producto. Todo depende de los requerimientos que sean identificados en la estructura de la red a proteger.

Una vez analizada cada una de las características principales de un IDS, ya se puede dar el siguiente paso, que es escoger el IDS apropiado que se ajuste a nuestra estructura de red y nuestros requerimientos.

La opción de escoger soluciones IDS de código abierto y considerando todas estas características mencionadas anteriormente, Snort, es un IDS que puede ser implantado en nuestra estructura de red.

Por ser de código abierto, existe la facilidad de personalizarlo al nivel que sea necesario, a diferencia de las soluciones comerciales que ofrecen otros proveedores de manera muy cerrada y sin tanta facilidad de personalización, pero todo esto se debe siempre tomar en cuenta, que depende de nuestros requerimientos.

3.2.4 Herramientas de monitoreo (logs)

Los logs son usados para un sinnúmero de cosas. Ayudan a resolver problemas, pueden ser usados para rastrear anomalías en una red, pueden ayudar a seguir los pasos de un intruso, o en otros casos ayuda a fortalecer aquellas debilidades no solucionadas.

Lo más importante al usar estas herramientas, es necesario contar con una estrategia, que a continuación detallaremos.

La forma más fácil de alcanzar una estrategia de logs es, escribir los logs en dispositivos, o copiar estos archivos a un servidor seguro.

Otra medida, es conectar a un puerto serial de una maquina a otra para enviar los logs a ese dispositivo, generalmente este se realiza en entornos UNIX. Ciertamente estos modelos son seguros, pero no necesariamente son escalables.

Otro modelo, que es pequeño pero escalable es usando el protocolo *syslog*. Este es un servicio nativo en casi todas las plataformas UNIX y que algunos sistemas operativos lo han agregado a sus productos. Es decir que hoy en día muchas plataformas cuentan con este modelo.

Hay alternativas mas seguras que el servicio de syslog, como es la de que todos los dispositivos de la red mantengan un sistema de log centralizado.

Por ejemplo, los administradores pueden configurar a todos los hosts hacia el servidor logs centralizado y protegido, de esta manera se da al equipo de seguridad un solo punto al cual coordinar el log de los datos, como se muestra en la Figura 2

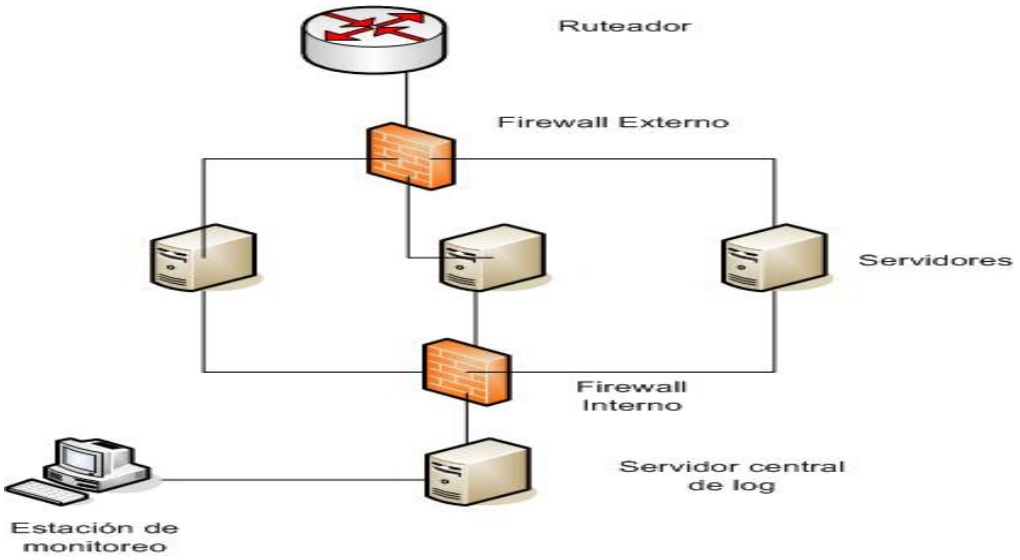


Figura 2 Log Centralizado

Cuando se configura apropiadamente, solo el tráfico permitido al servidor syslog, es destinado al puerto UDP 514.

Además en un log centralizado, se podría querer considerar el uso de al menos una herramienta de log de terceros. Esto tiene varias ventajas, primero; aunque muchos crackers y hackers son familiarizados con sistemas operativos basados en logs, pocos de ellos tienen conocimientos o saben evadir estos logs de terceros.

Segundo, los beneficios de los logs de terceros es que son independientes del sistema operativo. Entonces, se sabrá que intruso intentó penetrar al sistema comparando esta información con las herramientas establecidas inicialmente o con el log centralizado.

Esto es muy cierto, siempre y cuando se aísle el software log de terceros.

3.2.4.1 Búsqueda de vulnerabilidades

Existe software que sirve para buscar las vulnerabilidades de sistemas operativos instalados en una infraestructura de red. Busca las principales vulnerabilidades de los servicios que pueda estar prestando una aplicación en específico en los entornos operativos de una red. Actualmente existen dos clasificaciones principales en las vulnerabilidades de un sistema operativo, las cuales son; las expuestas a puntos locales o a nivel de host, y las que son expuestas a puntos remotos o a nivel de host remoto.

Para descubrir las vulnerabilidades a nivel de host remoto, existen algunos métodos para automatizar este tipo de tareas, tales como la búsqueda de puertos habilitados, la búsqueda del tipo de sistema operativo ejecutándose y otros más. Pero sin embargo, este tipo de búsqueda no detalla con exactitud el tipo de servicio que se está ejecutando, y por tanto no se podría saber la vulnerabilidad. Para encontrar la precisión en las vulnerabilidades, es necesario reunir los siguientes requisitos:

a. identificar que puertos del sistema están escuchando o habilitados
b. identificar la versión del servicio
c. indagar si hay alguna vulnerabilidad con respecto al servicio y la versión del mismo.

Una vez identificado cada uno de estos requisitos, se debería indagar por las posibles vulnerabilidades que puedan existir en los respectivos servicios, a fin de realizar las respectivas actualizaciones y parches de seguridad, o en su defecto, realizar la mejora del software o servicio.

Por lo tanto, se puede deducir que existen tres componentes principales en la búsqueda de vulnerabilidades, tales son:

Vulnerabilidad de datos.- Los sistemas de búsqueda de vulnerabilidades contienen bases de datos que ayudan a identificar los posibles huecos de seguridad que poseen los sistemas remotos.

Mecanismos de búsqueda.- Las técnicas que poseen estos sistemas, mantienen las capacidades para encontrar la información sobre servicios, sistemas operativos y las vulnerabilidades, todo esto depende de cómo fue diseñado el software, lo cual lo hará más eficiente para grandes grupos de PC's.

Mecanismos de reportes.- Algunos productos ofrecen fuertes maneras de manejar los reportes cuando encuentran problemas, en cambio hay otros que no poseen grandes fortalezas en sus reportes.

3.2.4.2 Criterios para escoger un buen buscador de vulnerabilidades

Para escoger un buen software de buscador de vulnerabilidades, se debe principalmente buscar los requerimientos necesarios que se van a aplicar en la infraestructura de red. Entre los principales criterios para tomar una buena decisión son los siguientes:[ANOM]

a.- Integridad de chequeos de vulnerabilidades.- Estos sistemas deberían conocer las vulnerabilidades más críticas en todos los niveles comprometidos en el sistema.

b.- Exactitud de chequeos de vulnerabilidades.- Es importante que estos sistemas tengan un gran set de chequeos de vulnerabilidades. Pero también es importante la exactitud con que identifican a estas vulnerabilidades.

c.- Alcance de chequeos de vulnerabilidades.- Estos sistemas principalmente debería buscar vulnerabilidades a sistemas remotos, pero en la actualidad existen mucho que ofrecen la búsqueda de vulnerabilidades a nivel de host locales. Existen otros que usan una agente para monitorear las vulnerabilidades para ambos casos, esta implementación es vista con gran expectativa en entornos muy extensos.

d.- Actualizaciones al día.- Este sistema debe siempre estar actualizado, con las últimas vulnerabilidades encontradas de todas las plataformas posibles, y con facilidades para obtener las mismas.

e.- Capacidades de reportes.- Es muy importante saber qué vulnerabilidades tienen los sistemas operativos y demás sistemas en una red, por ello es necesario la capacidad de generar reportes muy bien detallados, a fin de

encontrar con mayor facilidad las vulnerabilidades y así facilitar la búsqueda de los parches respectivos.

f.- Licenciamiento y precios.- Algunos sistemas son licenciados por hosts, por servidores y otros son gratuitos. Algunos tienen facilidades de licenciamiento y otros requieren de códigos de licenciamiento. Por tal motivo, se debe realizar un exhaustivo análisis de costos y licencias de acuerdo a los requerimientos de la infraestructura de red.

3.2.5 Antivirus

Hoy en día existen muchos virus, por tal motivo es siempre importante mantener un software antivirus, que permite mantener actualizado cada uno de sus motores de búsqueda de virus, a fin de mantener los sistemas completamente funcionales, ya que la infección de un virus podría provocar muchas pérdidas de dinero, por cuanto un sitio de ecommerce que no esté en línea provoca que no se compre nada. Ese tiempo de downtime, o fuera de línea es perjudicial para un negocio electrónico.

3.2.6 Sniffers

Son dispositivos que capturan paquetes de red. Su propósito es analizar el tráfico de la red e identificar potenciales áreas de interés para los intrusos.

Los Sniffers pueden variar en funcionalidad y diseño. Algunos sólo analizan un protocolo, mientras otros analizan cientos de protocolos. Pero hoy en día, la mayoría de sniffers analizan los siguientes protocolos:

- Ehernet estándar
- TCP/IP
- NetBios

Hay sniffers que tiene costos elevados, porque son especializados; mientras hay otros que son gratuitos, pero no ofrecen soporte.

Los sniffers son programas que siempre funcionan en modo promiscuo, es decir que capturan todos los paquetes en una red, sólo escuchan los paquetes, son agentes pasivos.

Los sniffers pueden representar un nivel de riesgo, por las siguientes razones:

- pueden capturar nombres de cuentas y contraseñas
- pueden capturar información confidencial
- pueden ser usados para obtener accesos a redes vecinas

Por lo tanto, un sniffer no autorizado en una red puede comprometer en un gran riesgo la seguridad.

3.3 Definición de políticas de seguridad

3.3.1 Importancia de políticas de seguridad

Las computadoras y las redes en una organización son muchas veces el componente que bosqueja la línea entre el éxito y las fallas de la compañía.

La seguridad sobre las computadoras y la Internet en nuestro trabajo diario, requiere de medidas de seguridad en todo nivel.

Principalmente en nuestro negocio, como lo es el comercio electrónico, las políticas de seguridad que se implementen en la infraestructura de red es primordial y es nuestro principal objetivo, a fin de evitar posibles fallas en nuestro servicio.

De tal manera que se definirán políticas en las siguientes categorías como son: el acceso físico a los equipos de comunicación y servidores, el acceso a cada host de la infraestructura de la red.

3.3.1.1 Acceso físico

El acceso hacia los equipos de comunicación, los servidores y estaciones de trabajo que se estén utilizando en la infraestructura de red, es necesario que sea solamente por el personal capacitado y específicamente quienes realmente deban acceder al mismo, quienes serán siempre los administradores. Por tal motivo, siempre el espacio donde se ubiquen estos equipos debe estar protegido, es decir que deben estar en un entorno

adecuado para tal operación, contar con puertas de acceso, con seguridades en cada una de ellas, a fin de evitar que cualquier persona entre al mismo.

Así de esta manera se puede evitar que alguna persona mal intencionada pueda conectar una PC y conectarse a algún switch de comunicaciones y puede usar algún tipo de ataque contra los servidores o servicios que se prestan, o aún puedan escuchar los paquetes de red que se estén transmitiendo.

Por lo tanto, como norma y política de seguridad, se debe identificar la persona que desea ingresar al sitio destinado para la infraestructura de red, antes de proceder a realizar cualquier cambio, a fin de evitar riesgos de fallas.

3.3.1.2 Acceso a los hosts

El acceso a los hosts en la infraestructura de red es también importante como los demás accesos, por ello es necesario definir exhaustivas políticas de seguridad a nivel de hosts, es decir a nivel de cada uno de los servidores y equipos de comunicación en la infraestructura de red.

A nivel de hosts, específicamente en los servidores, sólo deben tener acceso al sistema operativo los usuarios administradores, para esto; es necesario crear un usuario adicional, es decir crear un usuario nuevo al sistema con

privilegios de administrador, a fin de acceder con este usuario en caso de ser necesario.

También se debe considerar que es muy importante mantener una política de contraseñas seguras, es decir, establecer un estándar o una política de asignación de contraseñas en cada uno de los usuarios, servicios que sean utilizados en cada uno de los sistemas, esto permitirá un mayor grado de complejidad al tratar de averiguar una contraseña por parte de un intruso.

Por ejemplo, determinar una cantidad mínima de caracteres y una cantidad máxima, mezclar números y letras mayúsculas y minúsculas, considerando además las políticas básicas de asignación de contraseñas, como es el no asignar palabras del diccionario, palabras de nombres propios, nombres de mascotas y demás. Mientras más compleja y más larga la contraseña, disminuye el riesgo de un ataque de un intruso.

Toda esta información de usuarios y contraseñas asignadas en los sistemas operativos de cada host y de servicios y demás configuraciones, se debe almacenar en una base de datos, y mantenerla en un lugar muy bien guardada y libre del acceso no autorizado.

Mantener a cada uno de los programas, sistemas operativos, software en general que se esté usando en la implementación del sitio, siempre deben

estar actualizados, es decir, contar con todos los parches de seguridad y parches críticos, mejoras, corrección de errores, etc.

Luego, otra medida de seguridad es desactivar todo aquel servicio en cada servidor, que no esté siendo usado para la implementación de nuestro sitio. Solo activar los estrictamente necesarios para el uso específico que se ha diseñado.

Si logramos mantener cada una de estas políticas en completo funcionamiento, aseguramos en gran parte a cada uno de nuestros hosts y cualquier elemento que participe en nuestra infraestructura de red.

3.4 Diseño de la contingencia de la red

En toda infraestructura de red que se implemente para cualquier servicio que se esté brindado con la misma, siempre debe existir un plan de contingencia, es decir, que debe existir al menos un plan completamente funcional que sirva para reemplazarse en el peor de los casos en que la infraestructura o parte de ella falle en un momento determinado por cualquier motivo que se presente.

Para el caso de nuestro negocio o sitio de pagos electrónicos, nuestro plan de contingencia cubre desde un servidor, los equipos de comunicación y los servicios brindados. De tal manera que este plan de contingencia demanda

gran cantidad de tiempo y trabajo, por lo tanto también costos de implementación.

Por ahora solo nos enfocaremos en el plan de contingencia de la red de comunicaciones de datos. A continuación mostramos una figura que contiene el diseño lógico de la red con la respectiva contingencia a la misma.

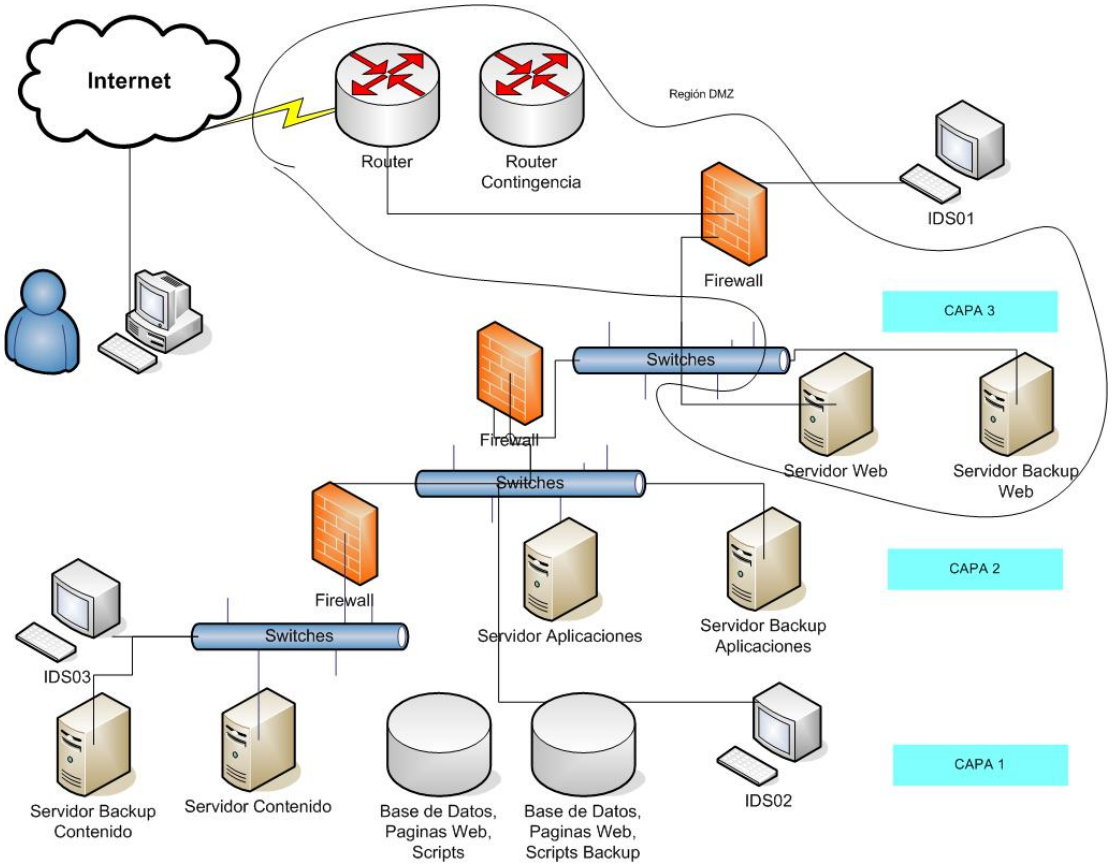


Figura 3 Diseño lógico de contingencia de infraestructura de red

La principal estrategia que usamos en el plan de contingencia, es la redundancia, es decir que en los equipos considerados más críticos para ofrecer nuestro servicio, se colocará un equipo igual o similar para implementar la redundancia. Esto se lo realiza con el propósito de que si falla

un equipo inmediatamente debe funcionar el redundante, y su funcionalidad debe ser completamente igual al equipo original, o al menos con los principales servicios que prestaba. Con esto se logra disminuir los costos por no operación del servicio, a pesar de que pueda ser muy poco tiempo el perdido, conlleva a problemas y principalmente el usuario final es quien se ve afectado por el mismo y eso se refleja como pérdidas en nuestro negocio electrónico.

En nuestro diseño lógico de la red de comunicaciones, en la región DMZ, se encuentra un ruteador con el que se tiene acceso hacia Internet, pero como parte de la contingencia debería existir otro igual, que también debe estar conectado hacia Internet como un respaldo de la comunicación, es decir que si sucediera algo con el ruteador primario, como daño de hardware, congestión de procesamiento debido a posible inundación de paquetes de red, o por cualquier otro motivo, debería entrar en ejecución el ruteador secundario, permitiendo así que la comunicación no se pierda, e incluso podría actuar como un balanceador de carga, es decir que este trataría de asumir la convergencia de las comunicaciones del ruteador primario, a fin de que las comunicaciones no se congestionen y mantener el servicio.

Asi mismo, en las conexiones que se realizan entre el proveedor de Internet y el ruteador, es decir si la comunicación es a través de fibra óptica, enlace radial, u otro tipo de enlace, también debe existir una comunicación de

respaldo, y a la cual el ruteador también debe tener las capacidades de soportar estas especificaciones.

Ya en la red interna, cuando la comunicación va ingresando hacia los posibles servidores, es decir, entre las divisiones de redes que se han configurado como se muestra en la figura anterior, existen los swtiches de capa 2, para los cuales también deben existir medidas de contingencia.

Una de las medidas a aplicar sería también la de contar al menos con un switch de similares características para ser reemplazado en cualquier momento en que uno de los dos llegase a fallar por cualquier motivo. Previamente este equipo debió ser configurado idénticamente al switch original, a fin de que en el momento del problema, simplemente se realice un cambio del equipo rápidamente e inmediatamente esté en línea.

Otra medida a tomar que depende mas bien del problema que le esté afectando a la red, específicamente al switch, tal como un daño ocurrido al puerto que está siendo usado por los servidores, la contingencia en este caso es simple, solo se debería cambiar a otro puerto disponible y funcional, y asignar las mismas políticas de seguridad a este como del puerto anterior.

Para la parte de cableado que exista entre las redes diseñadas en nuestra infraestructura de red, también se debe contar con una contingencia, es decir, si en caso de que los cables se dañen, se debe contar también con cables para su posible reemplazo. Aunque las probabilidades de que el

cableado estructurado se dañe son mínimas, por la calidad de los materiales y además la ubicación física de los mismos.

Podemos concluir que en este tipo de soluciones informáticas o negocios electrónicos, siempre se debe tener un plan de contingencia a todo nivel, para disminuir los costos por no operación del servicio.

3.5 Diagrama de red ideal

Para nuestro negocio electrónico se diseño una infraestructura de red en la cual existen todos los elementos necesarios e importantes, contando además con aquellos que fueron mencionados en el ítem anterior, es decir pensando en la contingecia.

Para una mejor optimización del servicio y a fin de proteger toda la información que se procesa durante una transacción que realice un cliente en nuestro sitio de pago electrónico, hemos diseñado nuestra infraestructura de red en tres capas a saber; capa 1 o de contenido, capa 2 o de aplicaciones y capa 3 o de servicios web.

A continuación describiremos cada una de estas capas.

3.5.1 Capa de contenido

En esta capa se ubica toda la información de los usuarios, de las transacciones, las páginas web del sitio y los scripts de aplicación.

Por tal motivo es muy importante mantener completamente protegida esta capa del acceso no autorizado de intrusos, ya que en esta capa es donde se ubicará a la base de datos, donde se registrarán las transacciones del negocio de nuestro sistema de pagos electrónicos.

3.5.2 Capa de aplicación

En esta capa se ubica toda la funcionalidad del sitio web o del sistema de pagos electrónicos. Aquí es donde se procesa toda la información de la capa inferior, para luego ser enviada a la capa superior, en donde el usuario final puede observarla.

Es decir, que es esta capa la que mantiene el dinamismo entre el usuario final y nuestro sistema de pagos electrónicos.

Por tal motivo también es importante que exista todas las seguridades al igual grado que la capa inferior, para siempre evitar el acceso no autorizado de intrusos.

3.5.3 Capa de servicios web

En esta capa es donde se presenta la información y que la publica hacia los clientes a través de la gran red de redes, Internet.

Esta capa no posee datos, solo los muestra, previamente la capa inferior los ha procesado para luego ser publicados por la capa superior.

Debido a que esta capa está mucho más cerca hacia al acceso de internet, y por lo tanto es más vulnerable al ataque de intrusos, es necesario que se apliquen estrictas políticas de seguridad, y por tanto se debe prestar la mayor concentración de seguridad, ya que es la principal puerta de acceso hacia las demás capas. Si se logra mantener protegida esta capa, por consiguiente las demás también se mantendrán protegidas.

A continuación se muestra el diseño anteriormente expuesto en la siguiente Figura 4.

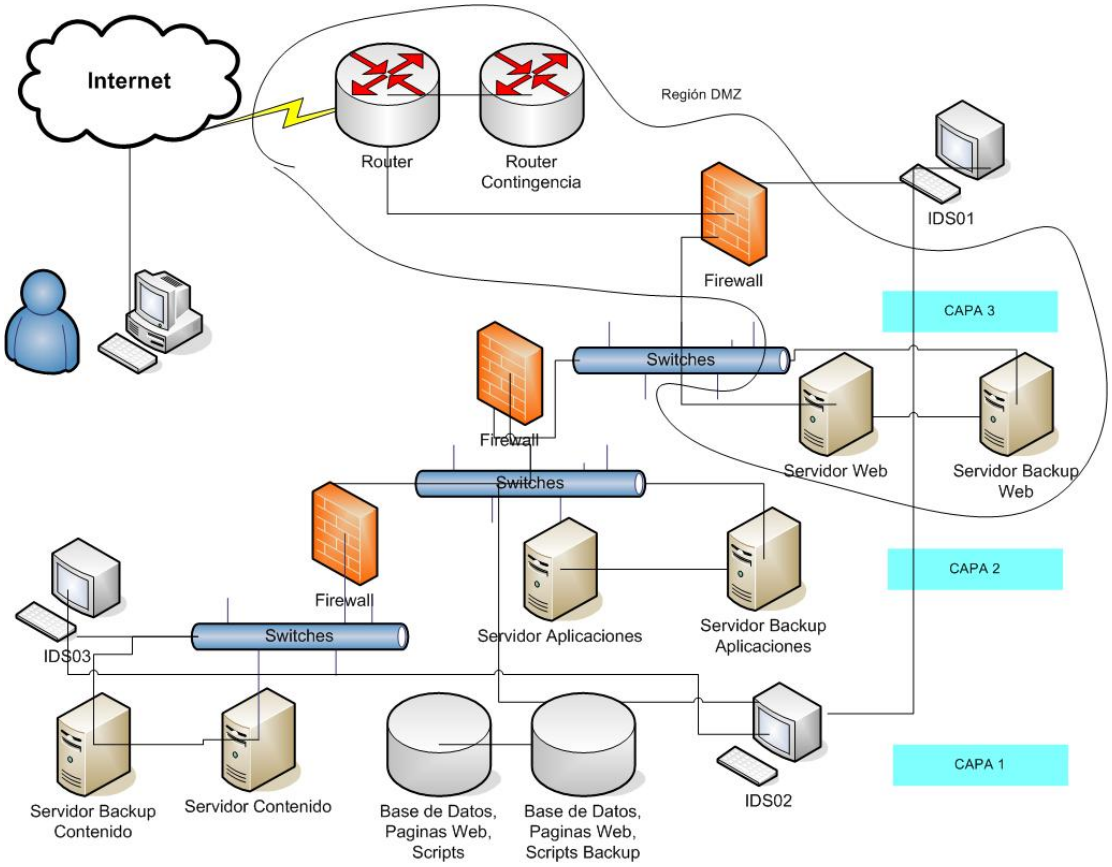


Figura 4 Diseño Ideal de la infraestructura de red

En esta figura también se muestra, que en cada capa existe la estrategia de contingencia, es decir que existen por ejemplo, en la capa de contenido existen dos servidores de bases de datos, de archivos. Así mismo en la capa de aplicaciones, existen dos servidores. Y así sucesivamente.

También en un futuro, es decir, en el caso de que los usuarios aumenten será necesario implementar una estrategia de distribución de carga para cada uno de los servicios que se prestan en cada capa, por tal razón este diseño es flexible a esos requerimientos, permitiendo así la facilidad de agregar otro servidor en la misma capa, sin necesidad de cambiar el esquema general.

En este esquema, también se puede observar que por cada capa se coloca un IDS, este actúa como un agente en cada capa, a fin de que reporte cualquier anomalía hacia un IDS central que se podría ubicar sobre la capa más superior, o que monitorea la capa de servicios web.

Entre cada capa se ha colocado un firewall para mantener protegida cada capa, con esto se está asegurando que solo se transmitirá el tráfico correspondiente a cada capa en ambas direcciones.

Por ejemplo, entre la capa de contenido y la de aplicaciones, solo debería transmitirse paquetes de acceso a la base de datos, de acceso a archivos, y de aplicación, y viceversa. Pero un paquete del protocolo http, no debería ser permitido entre estas dos capas.

Por lo tanto, solo se debería permitir el tráfico entre las dos capas relacionadas, y lo demás se debería bloquear.

De igual manera entre la capa de servicios web y el acceso hacia Internet, solo debería permitirse el tráfico generado por el protocolo http, ssl, y lo demás debería ser bloqueado, con este se establecería los respectivos niveles de seguridad en cada capa.

3.6 Diagrama de red ajustado

Para la implementación de nuestro proyecto, sólo hemos considerado dos de las tres capas que se plantearon en el diseño de la infraestructura de red, ya que la implementación del mismo, incurre en muchos recursos y por lo tanto no se puede contar con todos esos recursos que el diseño ideal lo requiere.

A continuación mostramos la figura con el diseño de red ajustado a nuestro proyecto.

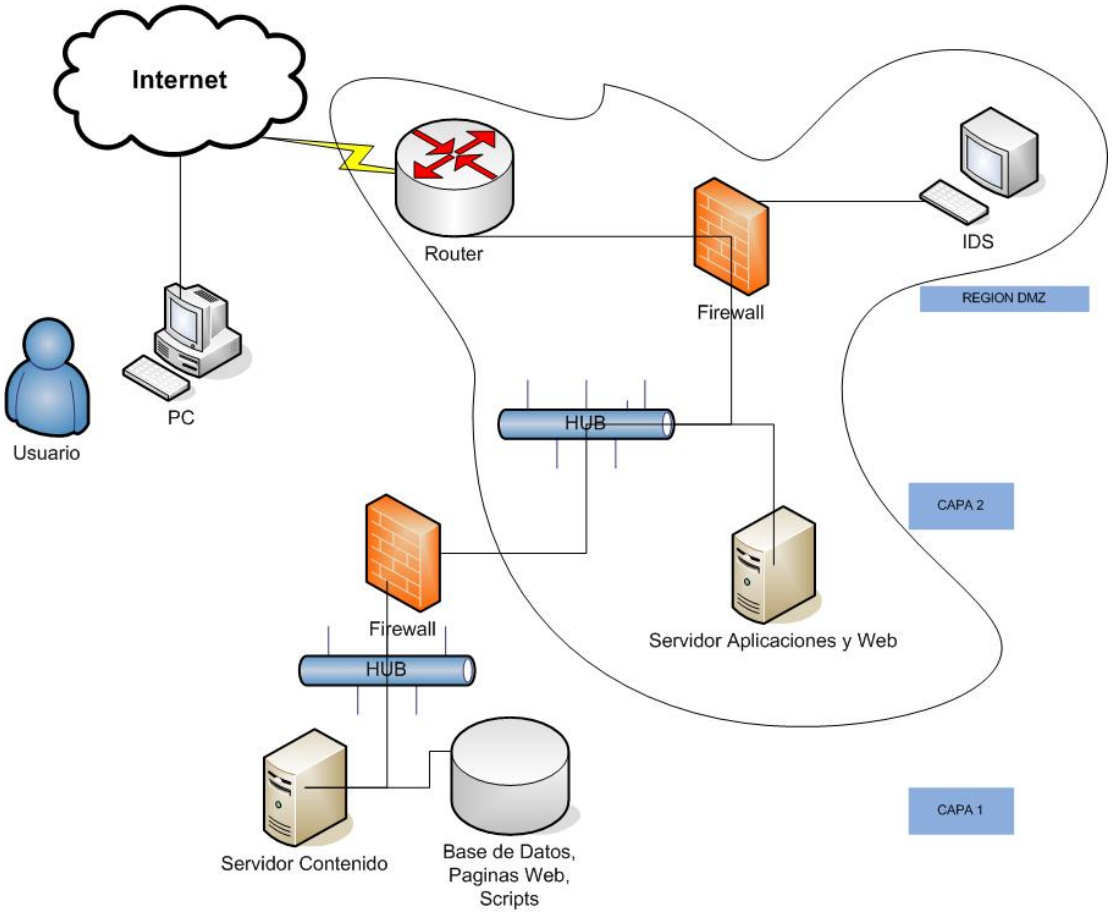


Figura 5 Diseño ajustado de la infraestructura de la red

En este diagrama mostramos solamente dos capas, la capa de contenido y la capa de aplicación y servicios web.

La capa de contenido, mantiene el mismo criterio, es decir, existe la base de datos, las páginas web y scripts de aplicación.

En cambio la capa de aplicaciones y servicios web, ambas se colocaron en una sola capa, por lo tanto se entiende que esta capa será igualmente mucho más protegida, como la capa solamente de servicios web.

De igual manera se conserva un firewall entre estas dos capas, a fin de sólo permitir el tráfico de protocolos de uso para la base de datos, sistemas de archivos compartidos.

Así mismo en la capa entre el servidor de servicios Web y el acceso hacia Internet, sólo se permitirá el acceso del protocolo http y ssl, lo demás deberá ser bloqueado.

Para el monitoreo de la red, se ha colocado principalmente un IDS en la capa de servicios web, a fin de monitorear el tráfico que acceda a este servidor y así poder tomar las medidas respectivas en cuanto a seguridad se refiera.

En los equipos de comunicaciones para dividir las redes hemos usado hubs y no swtiches como debería ser, y cada firewall realiza la función de un ruteador, para escalar las redes, por lo tanto, sólo se mantienen seguridades a nivel de cada host, es decir, que además de los firewalls de cada capa, cada servidor tiene configurado su firewall de host, establecidos con políticas de seguridad similares a los otros firewalls de red.

Por lo tanto, este esquema de red no es tan recomendable, pero si se configura a cada uno de los servidores y servicios de tal manera que no puedan ser interrumpidos, sí es una opción válida para la implementación de nuestro sistema de pagos electrónicos.

CAPITULO IV

IMPLEMENTACIÓN DE UNA RED SEGURA PARA EL HOSTING DE UN SITIO DE SISTEMA DE PAGO EN LÍNEA

4.1 Implementación de la infraestructura de la red

Para la implementación de nuestro sistema de pagos electrónicos en línea, nos basaremos en el diseño del esquema de red mencionado en el capítulo anterior, es decir el esquema ajustado de red.

Para lo cual usaremos todos los equipos mostrados en la Figura 5.

A continuación mostramos la lista de todos los equipos necesarios para esta implementación de infraestructura de red.

TIPO	DESCRIPCION
Servidor Contenido	Servidor que posee la base de datos, las páginas web, y scripts de aplicación
Servidor Web	Servidor que posee el servicio web y el servicio de aplicaciones
Servidor firewall 1	Firewall que protege entre la base de datos y el servidor web
Servidor firewall 2	Firewall que protege entre el servidor web y el acceso a Internet
Workstation IDS	PC que monitorea el acceso a las redes, sistema de IDS.
Ruteador	Sistema que de acceso a Internet y a la red interna
Hub 1	Conecta el segmento de la base de datos y el servidor web
Hub 2	Conecta el segmento del servidor web y el acceso a Internet

Tabla 8 Equipos utilizados en la infraestructura de red

Una vez establecidos todos los equipos necesarios, procedemos a realizar la configuración mostrada en la figura siguiente:

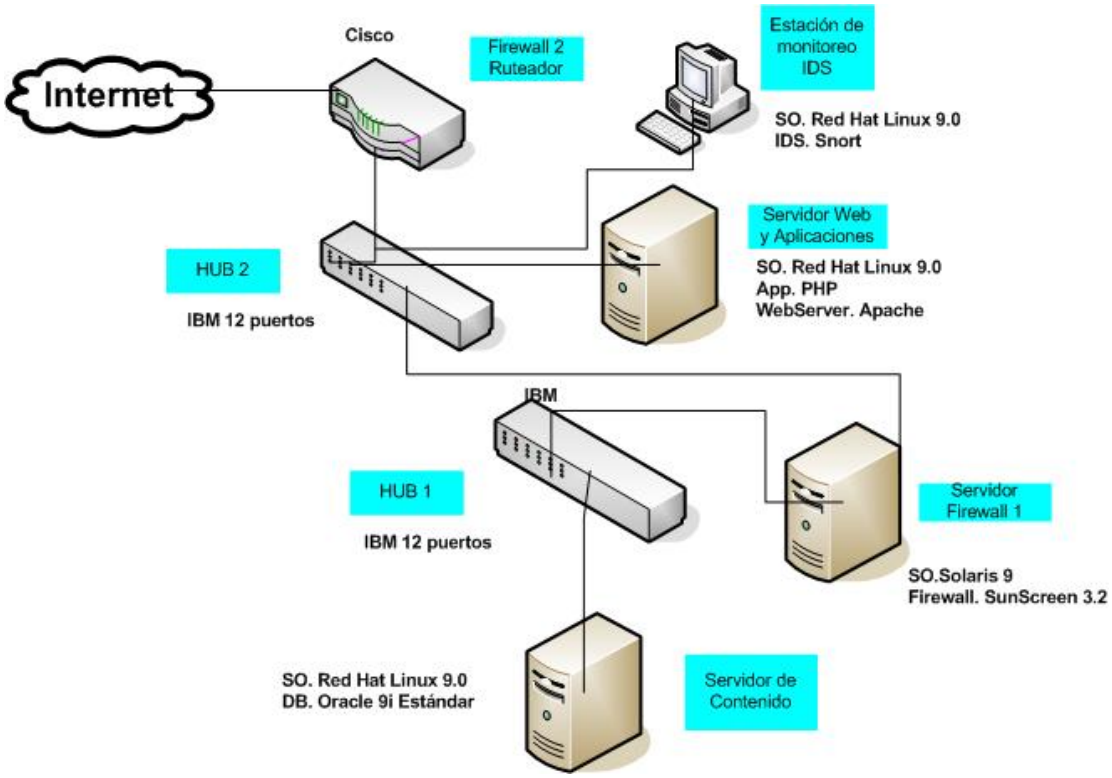


Figura 6 Diagrama Físico de la infraestructura de red

Como nuestro diseño se fundamenta en el criterio de dos capas, en el esquema físico también lo mostramos, y se lo realiza implementando dos redes diferentes. Tenemos por lo tanto lo siguiente:

CAPAS	REDES
CAPA 1 (CONTENIDO)	Red 192.168.1.0
CAPA 2 (WEB Y APLICACIONES)	Red 192.168.2.0

Tabla 9 Definición de Capas

Debido a que estamos colocando hubs entre cada red, quienes hacen de ruteadores para segmentar las redes, es decir, para rutear las paquetes de red que se comunican entre ambas redes, son los firewalls, que además de proteger ambas redes, también se les atribuye esta función de ruteadores.

Mas adelante mostraremos las configuraciones realizadas a estos firewalls.

4.1.1 Especificaciones técnicas de los equipos de red

A continuación mostramos en la tabla siguiente los equipos de transmisión de datos utilizados en nuestro proyecto.

DISPOSITIVO	MARCA	MODELO	PUERTOS	VELOCIDAD
Hub	IBM	8224	16	10 MB/S
Ruteador	CISCO	1751	2	10/100 MB/S

Tabla 10 Equipos de comunicaciones en la red

4.1.2 Configuración de la red

Hemos seleccionado redes de clase C para la identificación de nuestras redes privadas, es decir aquellas redes que no son públicas hacia la Internet.

Hoy en día el uso de redes de clase C, son las más usadas y generalmente son de uso privado y además por la gran cobertura que poseen para satisfacer grandes requerimientos de asignación de IP para muchos computadores o hosts en las redes.

A pesar de que nuestra infraestructura no requiere de tantas IP, si es importante mantener este esquema de direccionamiento IP para futuras

mejoras en nuestro servicio, especialmente cuando se deseen agregar mas servidores o equipos de comunicación.

Por lo tanto, como se había indicado anteriormente, en la capa 1 o de contenido, se asignó la red 192.168.1.0 con submáscara 255.255.255.0.

Luego, al servidor de contenido se le asignó la siguiente IP, 192.168.1.156, con sub máscara 255.255.255.0.

Este servidor se conecta hacia el hub 1 a través de un cable directo UTP. Además a este hub 1 se conecta el firewall 1 con la interfase 1, mediante cable directo UTP, cuya IP es la 192.168.1.128 con submáscara 255.255.255.0, de tal manera que esta interfase es la que actúa como ruteador para la red 192.168.1.0.

La capa 2 o de servicios web y de aplicaciones, está representada físicamente por la red 192.168.2.0. Aquí también se utiliza un hub, para lograr la comunicación entre el servidor web y la base de datos.

Por lo tanto, en el hub 2 se conecta el servidor web con cable directo UTP, cuya dirección IP del servidor es, 192.168.2.128 con submáscara 255.255.255.0 y también se conecta la otra interfase del firewall 1, con cable directo UTP, cuya dirección es 192.168.2.64 con submáscara 255.255.255.0.

A este hub 2 también se conectará una PC con el sistema de detección de intrusos, IDS para monitorear todo el tráfico que reciba el servidor web.

También se conecta una interfase interna del firewall 2, con cable directo UTP, que protegerá al servidor web del acceso a Internet, es decir, que este

equipo tiene la funcionalidad de ruteador de toda la red interna hacia Internet y a su vez protegerá del intento de acceso no autorizado.

La dirección IP de esta interfase del firewall 2 es 192.168.2.128 con submáscara 255.255.255.0, luego usando el protocolo NAT, o también conocido como Traducción de Direcciones de Red, la otra interfase, es decir la pública, tendrá dirección 200.10.168.25 y submáscara 255.255.255.0.

Por lo tanto, esta es la configuración que se realizó a esta infraestructura de red, y la cual es completamente funcional para que nuestro sistema de pagos electrónicos en línea funcione de manera apropiada.

A continuación especificamos las diferentes políticas de seguridad que se implementarán para mantener segura nuestra red y servicios.

4.2 Implementación de políticas de red

En esta infraestructura de red que hemos implementado, tenemos ahora que proceder a protegerla, es decir aplicar los principios de seguridad mencionados en capítulos anteriores, por lo tanto describiremos las políticas establecidas a nivel de host y a nivel de red.

4.2.1 Políticas establecidas a nivel de host.

A cada host de toda la infraestructura de red se definieron políticas de seguridad a fin de evitar posibles ataques o el acceso no autorizado, entre los cuales tenemos:

- Mantener actualizados y con los últimos parches a cada uno de los sistemas operativos usados en cada servidor y estaciones de trabajo.
- Mantener actualizados y con los últimos parches a cada una de las aplicaciones a ser usados durante el funcionamiento de la solución.
- Desactivar todos los servicios que hayan sido activados durante la instalación del sistema operativo de cada servidor, que no se vayan a usar para nuestros fines en nuestro sistema.

Es decir, que para nuestro servidor de contenido, donde reside la base de datos, solo deben estar activos los puertos TCP/IP que escuchan del servidor de base de datos, que en nuestro caso se atribuye a los puertos que Oracle usa para conectarse con sus clientes. Además, también debe estar activo el servicio de compartir archivos a través de la red, como es NFS (Network File System), adicionalmente los puertos para RPC, portmap, que son usados por los sistemas Unix. Los demás puertos que se puedan estar activos por algún servicio en particular, deben ser detenidos.

Para el caso de nuestro servidor web y de aplicaciones, solo deben estar habilitados los puertos que usa el protocolo http, como es el 80, el puerto 443 usado por el servicio de SSL (Secure Socket Layer), el puerto de NFS cliente, y los puertos de RPC para las comunicaciones entre el servidor web y el servidor de base de datos. Por lo tanto, todos los demás puertos y servicios que puedan estar habilitados, será necesario deshabilitarlos si no están en uso.

De igual manera se debe proceder en la configuración de los servidores que actúan como firewalls, es decir solo deberán estar activos los puertos que son usado por los firewalls y los demás deberán ser deshabilitados. Con mucha más razón se debe hacer énfasis sobre estos equipos, ya que son parte esencial en la infraestructura de red, ya que nos podrán defender de posibles intrusiones a nuestro sistema de pagos electrónicos.

4.2.2 Políticas a nivel de red

A nivel de red se deberán implementar las políticas de red que sirvan para evadir toda clase de ataques de los intrusos, por tal motivo en nuestro caso, ya que no usamos switches, sino hubs, no podemos implementar medidas de seguridad exhaustivas, pero lo que se debería hacer en este caso es simplemente evitar el que alguien pueda conectarse a uno de los puertos libres de los hubs y de ahí poder escuchar todo el tráfico generado en la red, por lo tanto, se deben considerar las políticas de acceso físico hacia los equipos de comunicación.

En cambio, si tuviéramos los switches, lo que se debería implementar, es que cada puerto libre del switch no sea activado a pesar de que cualquier PC se pueda conectar al switch, es decir no permitir conectarse, mientras el

administrador de la red no lo permita. De esta manera se protege al mismo switch y al resto de la red.

Asi mismo, el ruteador que se encuentra en la zona de acceso hacia Internet, deberá mantener políticas de seguridad mucho más estrictas, ya que solo permitirá el acceso al servidor web y el protocolo ssl,

Para proteger la transmisión de datos entre las redes, se colocaron los dos firewalls, de tal manera que solo irá el tráfico necesario hacia su destino, y viceversa.

En cada uno de los firewalls se han configurado una serie de políticas que son estrictamente necesarias para cada uno de los servicios configurados en las capas involucradas. Tal es el caso, de que el firewall 1 que protege a la capa de contenido o la red donde se ubica al servidor de contenido, solo permite el tráfico del servicio de la base de datos Oracle, el servicio de NFS, desde y hacia el servidor de aplicaciones y web, o la capa de servicios web.

De la misma manera, se aplican las mismas políticas en la dirección contraria, es decir desde la red de servicios web hacia la red de servicios de contenido.

Todas estas políticas que se han establecido en el firewall a fin de proteger los servidores de ambas redes, puede resultar ser similares con respecto a las políticas definidas a nivel de host, pero ambas son necesarias, ya que de

esta manera podremos mantener mucho mas seguro nuestros servidores y las redes en cuestión.

Por lo tanto, siempre se debería contar con políticas que se ajusten a los servicios estrictamente necesarios, y los servicios que no se usen, deben ser bloqueados o deshabilitados, con el propósito de que la red no esté vulnerable a posibles ataques dentro o fuera de la red interna.

4.3 Implementación de firewalls

Actualmente en el mercado informático, existen muchas soluciones de firewalls, y es muy importante saber escoger uno de ellos para ser tomado en cuenta en la implementación de nuestra infraestructura de red.

Para nuestra implementación usaremos los firewalls basados en red, es decir que protegeremos el tráfico generado entre redes.

Contamos con un firewall mediante software y otro firewall mediante hardware, ambos son completamente funcionales, y cumplen con las expectativas de nuestro proyecto.

Ambos firewalls que se utilizarán están basados en tecnología de packet filter, es decir el filtrado de paquetes de redes, por lo cual tenemos muchas opciones en el mercado, y a continuación realizaremos un análisis del producto seleccionado.

4.3.1 Comparación de productos firewalls

Entre los principales productos que hemos escogido para ser comparados tenemos, SunScreen de Sun, Firewall-1 de CheckPoint y NetScreen de NetScreen, los cuales son los principales y mayormente usados, específicamente para plataformas UNIX.

SunScreen de Sun, es un firewall muy versátil, que provee control de acceso, autenticación, y encriptación de datos. Además cuenta con un núcleo dinámico de filtrado de paquetes para el control de acceso a redes y también un núcleo de autenticación y encriptación de datos, para crear VPN con tecnologías de encriptación de clave pública. La administración es través de una interfase web segura, usando esquemas de encriptación. También se puede administrar a través de consola de comandos.

Para administraciones remotas, SunScreen soporta SKIP (Simple-Key Management for Internet Protocols) o IPSec/IKE (IP Security Architecture/Internet Key Exchange) para comunicaciones seguras entre la estación de administración y SunScreen.

Netscreen es un firewall basado en IVE (Instant Virtual Extranet), que permite obtener los beneficios manteniéndose en línea, posee políticas de seguridad y regulatorias, también reducen el riesgo de ataques al encarar la Internet.

Aplica fuertes esquemas de encriptación y autenticación, además de políticas de autorización y actividades de auditoria. Utiliza para la administración una sencilla interfase web.

La integración de este software con los demás componentes en una infraestructura de red no incurre en mayores costos.

El costo de este firewall NetScreen es mucho más elevado comparado con el SunScreen, ya que SunScreen es incluido como paquete adicional cuando se obtiene una licencia del sistema operativo Solaris, por lo que su valor es mucho más barato, a diferencia del NetScreen que es una solución específica y se vende como un producto separado.

Por lo tanto, una de las principales razones para escoger SunScreen como firewall para proteger nuestras redes es su fuerte integración con el sistema operativo Solaris, que por ser robusto nos brinda mayor confiabilidad y estabilidad en su funcionalidad, y por todas sus características adicionales de seguridad y además por su bajo costo de implementación.

4.3.2 Características para un servidor firewall

Debemos recordar, que nuestro firewall 1, es un firewall por software, por lo tanto, es una PC dedicado como servidor y además posee un sistema operativo basado en Unix como es Solaris.

Este sistema operativo fue escogido por sus grandes características como su robustez, seguridad, estabilidad, y escalabilidad.

Además, el hardware que se use para el servidor de firewall debe ser especializado, es decir, que debe poseer características de servidor, tales como, grandes capacidades de memoria RAM, de almacenamiento en disco

duro, velocidades altas de procesador; ya que es un sistema basado en el análisis de paquetes de red, y por lo tanto, debe contar con gran rapidez en el procesamiento de los datos.

Para lo cual mencionamos a continuación las características mínimas para un servidor que actúe como firewall.

CARACTERÍSTICAS	**MINIMO**
Procesador	SPARC o Intel
Velocidad	Intel 2.8 Ghz, SPARC
Memoria RAM	1 Gb
Disco Duro	40 Gb SCSI
Tarjetas de Red	3Com

Tabla 11 Características del servidor Firewall

Dependiendo del tipo de configuración que se vaya a implementar del firewall, es decir, en modo de routing o stealing, se podría especificar características adicionales.

Para utilizar un firewall se debe utilizar como mínimo dos interfases de red, y siempre se recomienda que sean de muy buenas características las tarjetas NIC, ya que estas deben soportar gran tráfico de paquetes de red, entre esas están las 3Com, Intel.

Pero si el firewall se lo configura en modo stealth, este servidor necesariamente debe poseer tres tarjetas de red o NIC, dos de las cuales servirán para el filtrado de paquetes y la otra servirá para la administración.

Básicamente la diferencia del modo de routing y el modo de stealing, está en que en el modo stealing, el firewall es transparente a la red que protege, es decir, es como si el servidor no estuviera conectado a la red, pero realmente si lo está.

Las características actuales de nuestro servidor son las siguientes:

ESPECIFICACIONES DEL SERVIDOR FIREWALL 1	
Procesador	Intel Xeon
Velocidad	1.2 Ghz
Memoria RAM	512 Mb
Disco Duro	36 Gb IDE
Tarjeta de red integrada	Intel PRO 10/100/1000
Tarjeta de red externa PCI	3Com 509

Tabla 12 Características servidor actual

Con este servidor, se procedió a instalar el sistema operativo Solaris 9 para plataforma Intel.

Luego se procedió a configurar al servidor según las políticas establecidas en cuanto al nombre del servidor, las direcciones IP de cada interfase, y demás parámetros de red necesarios para la configuración como firewall 1 en la infraestructura de red, como se muestra en la siguiente tabla:

Hostname	Srvfirewall01
IP interfase 1 (Intel)	192.168.1.128
IP interfase 2 (3Com)	192.168.2.64
Hostname interfase 1	Srvlan01
Hostname interfase 2	Srvlan02

Tabla 13 Parámetros de red del firewall 1

Una vez configurados todos los parámetros de red, se procedió a realizar la actualización de los parches de seguridad del sistema operativo.

Una vez realizadas estas actualizaciones, se procedió a instalar el software del firewall, para nuestro caso escogimos el SunScreen 3.2 para Solaris Intel, siguiendo todos los pasos previos a la instalación de este producto.

Luego de instalado, procedimos a configurar las políticas de seguridad que se habían establecido anteriormente a nivel de red, las cuales especificamos a continuación.

Origen	Destino	Protocolo	Acceso
Servidor web	Servidor contenido	Tcp oracle	Permitido
Servidor contenido	Servidor web	tcp oracle	Permitido
Servidor web	Servidor contenido	Tcp cliente nfs	Permitido
Servidor contenido	Servidor web	Tcp nfs server	permitido

Tabla 14 Politicas del firewall 1

Como norma de seguridad se cambió la contraseña del usuario “admin”, predeterminada del producto SunScreen a una nueva contraseña, a fin de

evitar posibles intentos de conseguir o tratar de adivinar la contraseña del administrador del SunScreen para adulterar las políticas establecidas.

Por lo tanto, este firewall 1 queda completamente configurado y probado para su funcionamiento indicado en el diseño.

En el apéndice se muestra las figuras de las pantallas capturadas del software firewall SunScreen, configurado de acuerdo a los requerimientos entre la capa de contenido y la capa web.

Para el firewall 2, que es el que va a proteger a la capa de servicios web y de aplicaciones del acceso a Internet, es decir la red donde se encuentra el servidor web y de aplicaciones, es un firewall por hardware, en este caso contamos con un ruteador, que a su vez hace de ruteador principal de acceso hacia Internet para toda la red interna.

Este es un equipo especializado para realizar tal función, de tal manera que no es un servidor como tal, pero tiene muchas características parecidas, pero recordemos que un ruteador, es una computadora también pero con una función específica.

Este firewall 2, en una de sus interfases se encuentra configurado hacia la red interna, cuya IP es 192.168.2.128 con submáscara 255.255.255.0 y la interfase externa hacia Internet cuya IP es 200.10.168.25 con submascara 255.255.255.0.

Luego mediante el uso de access-list, se implementan las seguridades y políticas necesarias para proteger la red interna.

Las access-list son la estructura básica del análisis de paquetes para realizar el filtrado, y permitir o negar que según el criterio establecido por el administrador, el destino de un paquete entre una interfase u otra, es decir para poder realizar la conmutación de paquetes mediante el filtrado.

El archivo de configuración de este router por hardware, se muestra en el apéndice.

Por lo tanto, en este firewall se definieron access-list específicas, en donde el tráfico que proviene de Internet requiere el uso del protocolo http que usa el puerto 80 es permitido pasar hacia el servidor web, asi mismo el tráfico del protocolo ssl, cuyo puerto es el 443. Todas estas access-list que se definan deben estar ubicadas en la interfase de entrada o la que se conecta hacia el Internet.

Por lo tanto, los demás puertos deberían estar negados, para evitar las posibles intrusiones.

Luego, para la interfaz de red interna, en cambio se debe permitir el acceso desde el servidor web hacia Internet, de los mismos protocolos como http, y ssl, a fin de que la comunicación sea completa y sin interrupciones. Aquí se debería especificar estas access-list, en esta interfase.

4.4 Implementación de Detección de Intrusos

Los IDS, Sistemas de Detección de Intrusos, son parte complementaria en una infraestructura de red, y principalmente en la nuestra, por medio del cual se podrá mantener un historial de toda actividad a través de cada red, que se vaya registrando, de tal manera que se pueda consultar y sirva para realizar las respectivas investigaciones o análisis en el caso de un intento de intrusión a nuestros sistemas.

En nuestro diseño ideal, especificamos que una buena solución de rastreo e historial de acceso a nuestras redes, es mantener un sistema de detección de intrusos a nivel de redes, es decir, que se debería colocar un IDS en cada una de las capas, o en cada una de las redes, de tal manera que se pueda monitorear cada una de ellas.

Esta herramienta es muy importante, ya que nos permitirá obtener datos casi exactos de rastreo cuando un intruso intentar acceder a cualquiera de nuestras redes, a fin de tomar las respectivas medidas de protección, y seguridad.

Aun después que llegase a suceder un hecho como la intrusión, mantener el rastro completo de este intruso, y proteger esta información hasta que este intruso sea detectado, y más aún que él mismo no intente manipular esta información.

Lograr esta implementación demanda de recursos adicionales, es decir que si colocamos un agente de IDS por cada red, significa que deberíamos colocar tres sistemas, uno para la red de contenido, otro para la red de aplicaciones, y otro para la red de servicios web.

Por lo tanto, deberíamos contar con tres estaciones de trabajo, cada una con software especializado en sistemas de detección de intrusos.

Dependiendo del software y del equipo de estaciones que se escojan, la solución de IDS puede resultar un mayor costo adicional a nuestra infraestructura de red.

Actualmente existen IDS de código abierto y gratuito, lo cual disminuye el costo de implementación de un IDS, solo sería necesario el hardware de las estaciones para instalar el software IDS y monitorear cada una de la redes.

Para la implementación de nuestra infraestructura de red, contamos solamente con un IDS, el cual será colocado en la red de servicios web y aplicaciones, es el punto entre el acceso hacia Internet y hacia el servidor web, y por tal motivo es muy importante mantener un constante monitoreo a fin de controlar el acceso o intentos de bloqueo de nuestro servicio.

Este nos ayudará a rastrear las posibles anomalías en esta red. Si logramos mantener la eficiencia de monitoreo en este punto, las demás redes podrán mantenerse protegidas, y por lo tanto estamos prescindiendo de colocar más IDS en la otra red.

Pero para equilibrar la situación de no contar con un IDS a nivel de red, hemos configurado cada uno de los servidores de las demás capas para monitorear sus servicios y eventos a nivel de host, es decir que existirán IDS a nivel de host, esta medida es también importante para nuestra infraestructura, ya que se mantendrá registro de los eventos que suceda en cada host.

4.4.1 Especificaciones de un IDS

A continuación detallamos las especificaciones técnicas recomendadas para la implementación de una estación IDS. Esta es una estación, no necesariamente un servidor.

ESPECIFICACIONES PARA UN IDS	
Procesador	Intel Pentium IV
Velocidad	1.2 Ghz
Memoria RAM	512 Mb
Disco Duro	30 Gb IDE
Tarjeta de red externa PCI	3Com

Tabla 15 Características para una estación IDS

4.4.2 Comparación de software ids snort y acid

El IDS más usado hoy en día es Snort, principalmente por ser de código abierto, y ya que además es muy estable y seguro.

ESPECIFICACIONES	
SNORT	ACID
Capacidad de monitoreo en tiempo real y análisis de trafico y paquetes	Capacidad de análisis de tráfico y paquetes
Capacidad de análisis de protocolos	Interface sencilla y construcción de querys
Basado en búsquedas y comparaciones para detectar ataques	Visualizador gráfico de paquetes de capa 3 y capa 4
Investiga y detecta sobrecarga de buffers, escaneo de puertos, ataques de scripts CGI, SMB, intentos de fingerprint y más.	Administración de alertas, logs.
Usa un lenguaje de reglas flexibles	Generación de gráficos estadísticos
Capacidad de alerta en tiempo real	
Compatible con varias plataformas	

Tabla 16 Comparación de IDS

Considerando todas estas características del software, es por ello que se lo considerada uno de los mejores IDS gratuitos y fáciles de implementar, y bastante seguro, que permite rápidamente encontrar posibles intentos de intrusión.

4.4.3 Configuración de Snort como IDS

Usando a Snort como software para la implementación de IDS basado en red, lo hemos instalado en la estación y usando como plataforma el sistema operativo Linux, ya que ambos son altamente compatibles y estables.

Se lo ha configurado de tal manera que se pueda monitorear la red donde se encuentra el servidor de web y de aplicaciones. El archivo de configuración del IDS, se lo muestra en el apéndice.

4.5 Implementación de servicio de antivirus para estaciones y servidores

Una muy importante medida de seguridad para defendernos de los molestosos virus informáticos, es usar plataformas de sistemas operativos como Unix. Los cuales no son muy susceptibles al ataque de virus, troyanos, backdoors, etc; pero sí es necesario para evadir intentos de realizar acciones maliciosas sobres las estaciones y servidores.

A continuación realizaremos un análisis de las soluciones antivirus existentes en el mercado.

4.5.1 Comparación de antivirus f-secure y trend-micro

En la actualidad, estos dos antivirus son los más usados y más populares en la protección de antivirus a nivel de host y de servidores.

ESPECIFICACIONES	
F-SECURE	TREND-MICRO
Protección sensitiva, comprensiva y flexible	Capacidades de alta efectividad de anti-spam
Confiabilidad	Soporte para crecimiento de la infraestructura
Rendimiento mejorado y superior	Protección comprensiva
Linea de comandos para escaneo mejorada	Protección de emails
Protección automatizada mediante scripts usados en el cron	Interface web intuitiva
Actualizaciones automatizadas	Facilidad de administración

Tabla 17 Comparaciones de Antivirus

Basados en nuestros requerimientos, y en las características de ambos productos, hemos escogido F-Secure como antivirus para la protección de nuestros servidores, además por ser un producto que nos brinda mayor garantía en cuanto a la protección en plataforma Unix, a diferencia del otro que recientemente incorpora soporte para plataforma Unix.

Con el antivirus seleccionado, como es el F-Secure, hemos procedido a proteger nuestras estaciones y servidores, de tal manera que podamos

mantener segura la información de cada uno de ellos, esta acción siempre se debe tomar indiferente de la plataforma de sistema operativo que se escoja.
Por lo tanto, toda estación y servidor se mantendrá protegida y segura con un software antivirus, con esto se contribuye a la seguridad de nuestro sistema de pagos electrónicos.

4.6 Implementación de servicio de antivirus para correo electrónico

En nuestro sistema de pagos electrónicos usamos el servicio de correo electrónico, por medio del cual logramos comunicarnos con nuestros clientes, indicándoles cada una de las transferencias, depósitos, retiros, u otra transacción que se realice en nuestro sitio y que el usuario necesite saberlo. Además, los usuarios o nuestros clientes, tienen la oportunidad de enviarnos correos electrónicos y por lo tanto, debemos estar protegidos a cualquier eventualidad que pueda presentarse a través de este medio.
Por tal razón, en nuestra infraestructura contamos con un servidor de correo que también se debe ubicar en la capa de servicios web, es decir, que debe estar lo más cerca al acceso a Internet, para que todo mensaje que es recibido o enviado sea alcanzado.
Para nuestra infraestructura, hemos configurado nuestro servidor de correo electrónico en el mismo servidor de servicios web y aplicaciones, debido a la optimización de recursos en nuestro proyecto.

Por lo tanto, procedimos a instalar el software antivirus disponible para nuestra plataforma, de tal manera que proteja todos los correos entrantes y salientes de nuestro servidor y así garantizar la seguridad de los correos electrónicos.

Con esto garantizamos que sólo usaremos la información válida para nuestros clientes y hacia ellos. Considerando que el contenido de la información transmitida por medio de los correos electrónicos hacia nuestros clientes, necesariamente no es clave para nuestros sistemas, es decir que su contenido es solamente informativo para el usuario o cliente que utilice nuestro servicio. Por ejemplo, cuando un cliente realice una transferencia de una cuenta virtual hacia otra cuenta virtual de otro cliente, el sistema enviará un correo electrónico para indicarle al usuario de la que transferencia fue realizada exitosamente. Es decir, información al instante.

Por lo tanto, como nuestro correo electrónico implementado en nuestro servidor web y de aplicaciones, está también ubicado el servidor de correos electrónicos, que para nuestro caso usamos una implementación que existe o es parte del sistema operativo Linux, como es el sendmail. Un producto muy usado por grandes empresas y usuarios avanzados, de gran utilidad y grandes beneficios.

Siempre se deben considerar las últimas versiones de este software, para evitar posibles agujeros abiertos que puedan utilizar los intrusos para tratar de adulterar la información de nuestros correos.

Lo más importante siempre es mantener actualizado nuestro software de administración de correo electrónico.

Por razones de seguridad, sendmail está configurado para ser utilizado solo con el protoclo SMTP (Simple Mail Transfer Protocol), ya que se enviará y recibirá correos mediante este protocolo.

Sus demás protocolos, como el POP, IMAP, será deshabilitados, ya que no estamos prestando servicios abiertos de correo electrónico, solamente para interacción entre el usuario final y nuestro sistema.

Este mecanismo de interacción entre un usuario y los sistemas basados en web, mediante correos electrónicos, o también sistemas de autorespuesta de correos, es también conocido como Mail Robots. Los cuales realizan tareas automáticas de envío y recepción de correos electrónicos.

En nuestra implementación existe una pequeña parte del uso de esta definición, es decir, que no necesariamente es un sistema de autorespuesta automática, porque para nuestro sistema, cada vez que el usuario realice una transacción, el sistema genera el correo electrónico correspondiente, y el sendmail se encarga de enviarlo a su destinatario.

Por lo tanto, el uso de mail robots será muy útil para ciertos sistemas, hoy en día es muy usado a pesar de que existen pocas soluciones web que lo utilicen. Pero su futuro será muy bueno, especialmente en áreas como el comercio electrónico.

4.7 Implementación de servidor de Base de Datos

En nuestro sistema de pagos electrónicos en línea, debemos contar con una base de datos que cumpla con las principales características de sistemas de servicios web, es decir que sea robusta, segura, compatible, de alta disponibilidad, eficiente, con garantía y soporte.

De tal manera que siempre preste el servicio, es decir, con soporte a tolerancia a fallos, que muchas de las tareas tradicionales en una base de datos puedan ser realizadas durante su actividad normal, si necesidad de que la base permanezca fuera de servicio por mucho tiempo.

Estas características deben buscarse en una base de datos para nuestro sistema, ya que es la parte más importante de todo lo demás componentes que comprende nuestro sistema. Es aquí donde se almacenará todas las transacciones que realice el usuario.

4.7.1 Comparación entre oracle y sqlserver

La base de datos es uno de los componentes muy importantes en nuestra infraestructura de red y en la solución de negocios. Por ello es necesario que

la base de datos cumpla con los requerimientos para la implementación de nuestro sitio.

Realizaremos la comparación entre las bases de datos más populares en el mercado como son Oracle y Sql Server.

ESPECIFICACIONES	
ORACLE	SQL SERVER
Alto desempeño de servicios como DW, ETL, OLAP	Herramientas de fácil utilización para los negocios
Comprensivo	Capacidades de administración y rendimiento
Acceso abierto a servicios web a través de SQL, Java, XML	Servicios y aplicaciones de administración de datos
Tolerancia a fallas de humanos, desastres, fallas del sistema	Escalabilidad
Reduce costos de administración de usuarios	Análisis avanzado de datos
Protege la integridad de los datos	Disponibilidad
Seguridad	Seguridad
Privacidad	
Costo efectivo de administración en un 30%	
Multiplataforma	Plataforma Windows

Tabla 18 Comparación de bases de datos

En esta tabla se observa que ambas tienen características muy similares, pero Oracle ofrece mejores características en cuanto a seguridad y robustez

en varios sistemas operativos. Principalmente en sistemas Unix, a diferencia de SQL Server, solo sirve en plataformas Microsoft.

Si comparamos los costos de la base de datos, es decir del software, realmente Oracle es un poco más cara, pero tiene mucho valor agregado al adquirir este sistema, y una gran línea de soporte.

Como nuestro proyecto, usa en el servidor destinado como base de datos el sistema operativo Linux, se utilizó una versión de Oracle la 9i con soporte para Linux, de tal manera que se pueda implementar una base de datos segura y mantenga la integridad de los datos y fuera de riesgos de acceso no autorizado.

Una vez seleccionada la base de datos que será implementada en nuestro sistema, procederemos a la respectiva instalación de la misma.

Siguiendo el esquema de uso de plataformas de sistema operativos de código abierto, como es Linux, se procedió a instalarlo en el respectivo servidor, para que de soporte a la base de datos.

A continuación se detallan las características mínimas para un servidor que cumpla la función de servidor de bases de datos.

ESPECIFICACIONES MINIMAS PARA UN SERVIDOR DE BASES DE DATOS	
Procesador	Intel Xeon
Velocidad	1.8 Ghz
Memoria RAM	2048 Mb

Disco Duro	36 Gb SCSI en configuración RAID 5
Tarjeta de red externa PCI	3Com

Tabla 19 Características para un servidor de base de datos

Esta es una configuración básica de un servidor típico para base de datos, dependiendo del presupuesto y el alcance que se haya planteado para este sistema, se puede aún más mejorar la configuración o disposición del hardware para este servidor. Es decir, si es necesario de grandes cantidades de almacenamiento de datos, o sea, discos duros de grandes capacidades, de tecnología SCSI, y también configuraciones de arreglos de discos RAID, los cuales también presentan tolerancia a fallos a nivel de discos duros, de tal manera que se pueda recuperar la información tan pronto como se pueda.

También se debería incluir grandes cantidades de memoria, que generalmente se lo hace para sistemas que permanecen en línea las 24 horas del día, tal es el caso como de los servicios web.

Para nuestro proyecto, hemos considerado una simple PC con ciertas características que permitan la instalación de la base de datos que se practica para nuestro caso. A continuación los detalles.

ESPECIFICACIONES	
Procesador	Intel Pentium III
Velocidad	1.0 Ghz

Memoria RAM	320 Mb
Disco Duro	30 Gb IDE
Tarjeta de red integrada PCI	SiS

Tabla 20 Características del servidor de base de datos usado

Luego, en este equipo se instaló la base de datos Oracle, versión 9i para plataforma Linux. Se realizaron las respectivas actualizaciones referentes, instalación de parches, y demás.

Una vez realizado el análisis y diseño de la base de datos, se generó el script de creación de la respectiva base para nuestro sistema de pagos electrónicos. Se crearon todos los objetos como tablas, indices, triggers, procedimientos, que serán utilizados durante el funcionamiento de nuestro sistema.

En el servidor de bases de datos, también se consideró durante su instalación, medidas de seguridad en cuanto a posibles fallas en los sistemas de archivos del sistema operativo, es decir, que el lugar donde se almacena la información de la base, están en directorios específicos que no son del sistema operativo, para evitar riesgos de fallos, en el caso de que el sistema operativo falle y pueda ocasionar daños a la base de datos. De tal manera que en el peor de los casos, solo sea necesario reinstalar el sistema operativo y luego configurar la base de datos nuevamente, pero con los datos completamente íntegros.

Por lo tanto, este servidor deberá estar protegido y siempre en constante monitoreo a fin de evitar posibles intentos de acceso no autorizado.

4.8 Implementación de seguridades de la Base de Datos

Además de que esta base presenta seguridades en su estructura, es decir, cubre todos los posibles huecos de seguridad, también se deben analizar todos los servicios que tiene activados de manera predeterminada.

De tal manera, que solo debe estar habilitado los servicios o puertos TCP/IP para escuchar a los clientes que se van a conectar a la base, como en este caso, el cliente es el servidor web y de aplicaciones.

Porque esta versión trae habilitados puertos de su propia aplicación, servidor web, y otros servicios que no son necesarios para nuestra implementación.

Además, consideramos la protección a nivel de host, es decir, que se ha configurado el firewall que viene integrado con el sistema operativo, con el propósito que solo permita conexiones de entrada y salida que realicen un requerimiento a la base de datos desde el cliente, mientras que el tráfico que no cumpla con estas especificaciones será negado.

Debemos recordar también, que este servidor que se encuentra en la capa de contenido, cumple otras funciones adicionales, como es el de servidor de archivos, donde residen las páginas web estáticas y dinámicas, y los scripts de aplicación.

Por lo tanto, para usarlo como servidor de archivos, lo hemos configurado a través del protocolo o servicio NFS, es decir que este es un servidor NFS, de tal manera que es necesario compartir los directorios que serán usados por los clientes.

Para nuestro caso, sólo compartimos dos directorios, que son el directorio de la base de datos, y el directorio del sitio web.

En el directorio de la base de datos, se encuentran los archivos ejecutables de la base, que son necesarios para ser accedidos por el cliente solo para lectura, durante la configuración de la aplicación e integración con el servidor web.

Mientras que el otro directorio compartido que es el del sitio web, es decir, donde se alojan todas las páginas web del sitio, se tendrá el acceso con control total para el cliente, ya que por configuraciones dinámicas en los sitios web, es necesario que exista esta facilidad para actualizar una página.

Todas estas funcionalidades establecidas en este servidor son controladas por el firewall del servidor, de tal manera que sólo estará permitido al cliente realizar estas operaciones, caso contrario se restringirá.

Así mismo el firewall que se encuentra ubicado entre ambas redes, considera también cada una de estas configuraciones de tal manera que se cumpla con el objetivo de proteger al máximo nuestro servidor de bases de datos.

Por lo tanto, siempre se deben considerar todos estos aspectos a nivel de la base de datos, e incluso el usuario que tenga acceso a todos los objetos de la base, debería poseer una contraseña segura, es decir, que no sea tan fácil de descifrar.

En el apéndice se muestra los accesos, privilegios y controles para los usuarios que usa la aplicación web para interactuar con la base de datos.

4.9 Implementación de seguridades en el servidor web

En toda solución informática que esté orientada hacia el uso de Internet como un servicio, el componente principal a protegerse, es el servidor web y de aplicaciones.

Es aquí donde muchos intrusos y hackers ponen toda su atención para tratar de que el sitio sea saturado, o de que el sitio en algún momento permanezca fuera de línea. Lo cual representaría una pérdida para el negocio.

Por lo tanto, este servidor web debe estar configurado de tal manera que preste todas las seguridades y protecciones necesarias a fin de que no pierda el servicio y mantener a los clientes satisfechos y seguros de sus transacciones que realicen.

4.9.1 Características de un servidor web

A continuación detallamos las características principales de hardware para que cumpla la función de servidor web:

ESPECIFICACIONES PAR UN SERVIDOR WEB	
Procesador	Intel Xeon
Velocidad	2.4 Ghz
Memoria RAM	2048 Mb
Disco Duro	40 Gb SCSI
Tarjeta de red PCI 10/100/1000	3Com

Tabla 21 Características de un servidor web

Con estas características se podrá implementar el hosting para un sitio web que soportará la demanda de un sistema de pagos electrónicos. Dependiendo de la demanda de usuarios o clientes, en un futuro se podría pensar en varios servidores web que compartan la carga, de tal manera que se distribuya la carga de los clientes web, hacia los servidores web y así permitir el acceso rápido y garantizado de todos estos usuarios.

Para nuestro caso, hemos implementado en un servidor la instalación del servidor web y de aplicaciones, el servidor posee las siguientes características:

ESPECIFICACIONES DEL SERVIDOR WEB	
Procesador	Intel Pentium II
Velocidad	500 Mhz
Memoria RAM	320 Mb
Disco Duro	30 Gb SCSI

Tarjeta de red integrada PCI	Intel

Tabla 22 Características de nuestro servidor web

Una vez que contamos con el hardware seleccionado para nuestro servidor, debemos proceder a la instalación de un sistema operativo.

Para cumplir con los objetivos de seguridad, confiamos en un sistema operativo que nos brinde todas las compatibilidades, estabilidad, escalabilidad, seguridad y fortalezas que se necesitan para brindar un servicio web.

Por tal motivo, hemos considerado que un sistema operativo basado en plataforma Unix cumple nuestras expectativas, ya que estos sistemas operativos no son tan vulnerables a los intrusos, como lo son otros sistemas operativos como Windows, que son más susceptibles a ataques de virus, intrusos, este es el favorito de estos individuos.

En nuestro servidor se instaló el sistema operativo Linux Red Hat 9.0 y se le realizaron todas las actualizaciones del caso, es decir se instalaron todos los posibles parches de seguridad al sistema.

Luego de esto, se procedió a configurar al sistema con solamente los servicios necesarios para su uso, como es el servicio de web, servicio de cliente de NFS, el servicio de SSL, y el de firewall a nivel de host.

4.9.2 Selección del servidor web

Actualmente existen muchas soluciones de servidor web disponibles en el mercado, pero basados en nuestra plataforma son más específicos. Existen servidores web basados en plataforma de sistemas operativos Windows, como el Internte Information Services, que es ampliamente usado.

Pero a nivel de plataforma Unix, tenemos varios servidores web de código abierto y gratuito como Apache, Caudium, etc, y también los hay aquellos que son de código cerrado o propietarios, como Sun Web Server de Sun incluido en el sistema operativo Solaris, WebSphere de IBM, etc.

El servidor de Windows, Internet Information Services, por ser el más usado en la mayoría de los sitios web, es también foco de ataques para la gran parte de los intrusos. En cambio los servidores web bajo plataformas Unix, son atacados también pero no en la misma intensidad que los demás sitios web basados en plataforma Windows.

Entre los servidores web basados en plataformas Unix, el más usado es Apache, por ser un servidor seguro, estable, escalable, y con soporte para grandes cantidades de conexiones y demás características funcionales del mismo, lo hacen el preferido a la hora de elegir un servidor web. Existen también otros servidores web, pero muchos de ellos son nuevos, recientes versiones, que no se puede medir la fortaleza de estos servidores web, a diferencia de Apache que ya tiene ganada esa ventaja con respecto a los demás en el mercado.

4.9.3 Comparación de apache con caudium

Apache es uno de los servidores web mas usado sobre plataformas Unix, en cambio Caudium es también un servidor web compatible con plataforma Unix, pero que se ha desarrollado recientemente, y tiene un crecimiento moderado de su uso.

Comparamos los dos, porque ambos son usados bajo plataformas Unix, y además ambos son de código abierto.

ESPECIFICACIONES	
APACHE	CAUDIUM
Soporta multiprocesos	Modo opcional de multiprocesos
Soporta multiprotocolos	Interfase web sencilla
Nuevas API	Permite creación de plantillas web
Filtrado de CGI	Flexibilidad, permite crear nuevos tags
Configuración mas sencilla	Configuración sin línea de comandos

Tabla 23 Comparación de servidores web

Estas son las principales características que ambos poseen, y por lo que apache se lo considera uno de los servidores web gratuitos más usados, además de su estabilidad, simplicidad y robustez, es preferido.

Por lo tanto, para nuestra implementación escogimos a Apache como nuestro servidor web.

4.9.4 Seguridades de apache

En vista de que vamos a usar como servidor web a Apache, hay que realizar las respectivas configuraciones adecuadas para mantener seguro nuestro servidor y nuestro sitio web, ya que este software es un recurso de código abierto.

Lo más importante en la seguridad de un sitio web, es que se debe restringir el acceso a las páginas web que no sean las solicitadas por el cliente browser, de tal manera que cuando se intente realizar cargar un página web de manera manual, sea restringido.

También se debe negar el acceso de intento de escritura sobre los archivos del sitio web, es decir que un intruso mal intencionado intente actualizar nuestras páginas web de tal manera que cambie nuestra información. Para esto, recordando que nuestro servidor web es un cliente NFS y que se conecta hacia el servidor NFS, está permito a este servidor con acceso de lectura al usuario que generalmente usa el servidor web Apache, como es “apache”. Este usuario solo tendrá privilegios de lectura sobre el servidor NFS y estará también restringido algún acceso al shell del sistema operativo.

Como medida de seguridad en la configuración de un servidor web, siempre se debe cambiar la mayoría de los parámetros que vienen predeterminados por el fabricante y también se debe deshabilitar aquellas configuraciones que estén habilitadas. Esto es muy importante ya que este uno de los principales

medios por lo cual los intrusos intentan buscar fallas en la seguridad del servidor web.

Una forma de mantenerse siempre actualizado en cuanto a las seguridades que puedan tener los servidores web, especialmente apache, es visitar con frecuencia el sitio web del fabricante del software, y mantenerse al día en las noticias de seguridad que sean publicadas. Y aplicar las respectivas actualizaciones en caso de existir.

Generalmente los hackers intentan realizar ataques de tipo DoS, (Denial of Service), es decir tratan de congestionar al servidor web provocando volcados de memoria y entorpecer las transacciones del mismo.

Otros de los intentos de ataque son las fallas en la autenticación, en que se trata de que el servidor autentique a usuarios no autorizados, por tal motivo no se debe crear usuarios con privilegios de administrador en este servidor.

Estas son las principales y más comunes medidas de seguridad que se deben tomar en consideración en el momento de implementar un servidor web con Apache.

4.9.5 Comparación entre php y asp

PHP es un lenguaje de scripts ampliamente usado por los desarrolladores web en sus páginas dinámicas, debido a su facilidad de embeber su código en el html. PHP (Hypertext preprocessor) es un lenguaje interpretado de alto

nivel, tiene una sintaxis similar a C y es muy fácil de aprender. Este lenguaje es compatible con muchas plataformas, como Unix, Windows.

ASP (Active Server Pages) es una aplicación creada por Microsoft, que trabaja sobre plataformas Windows. El código es ejecutado en el cliente y no en el servidor a diferencia de PHP, es también un lenguaje sencillo, pero su implementación no es de código abierto, mas bien esta aplicación viene incluida en algunos casos en los sistemas operativos Windows Server. Es decir, que está ligado al sistema operativo, el costo se incurre en el sistema operativo, a diferencia de PHP que es indiferente del sistema operativo.

ASP por ser un lenguaje que está incluido en sistemas operativos Windows y por tanto muy difundido en el mundo, los hackers o intrusos prefieren dañar a los sitios web que usen esta tecnología de aplicaciones, y este es uno de los principales motivos por el cual se escoge a PHP como lenguaje de aplicación, aunque tampoco no está libre de ataques, pero sí son menos.

Con PHP se pueden realizar múltiples tareas, no sólo la de páginas web dinámicas sino también aplicaciones gráficas, debido a que los scripts se ejecutan del lado del servidor y no del cliente, esto permite que sea más versátil.

Posee soporte para muchas bases de datos, entre ellas las más conocidas como Oracle, DB2, MySQL, etc a diferencia de ASP que no provee soporte para bases de datos sobre sistemas Unix, como Postgres, MySQL.

Además ASP, sólo se la utiliza para implementación de páginas web dinámicas, en cambio PHP se lo puede utilizar como aplicación no web, ya que se instala el intérprete y se ejecutan los scripts para que funcione la aplicación.

Ambos tienen soporte para varios protocolos como LDAP, POP3, SSL, etc, y también soporte para XML.

Por lo tanto, nuestro servidor de aplicaciones será PHP, de esta manera nuestra aplicación mantendrá un código seguro, y estabilidad entre las transacciones que se realicen.

4.9.6 Instalación y configuración de php

Para la instalación de PHP sobre nuestro servidor Web, es necesario tener disponible el software que vamos a utilizar, para nuestro caso debemos obtener el apropiado para que funcione sobre el sistema operativo Linux.

Para esto, lo obtenemos desde el mismo sitio web del fabricante como es www.php.net, bajar la última versión disponible y proceder a instalarlo en el servidor web.

Entre los archivos que viene en el comprimido del php, también existe un archivo de ayuda para la instalación, el cual se puede seguir para realizar instalaciones sencillas, pero para nuestro caso y por la configuración de nuestra infraestructura de red, es necesario realizar ajustes a la configuración durante la instalación del mismo.

A continuación mostramos las sentencias de instalación del php y que será integrado al servidor web que es apache y además la base de datos como lo es oracle.

Se debe ejecutar el siguiente script y con los siguientes parámetros:

./configure –with-oci8=/mnt/db/ --with-apxs2=/usr/local/apache2/bin/apxs/ --with-ldap/ --with-openssl=/usr/local/ssl –with-gd/ --with-jpeg-dir/ --with-zlib-dir/ --with-freetype-dir –with-png-dir/ --with-xpm-dir/ --enable-gd-native-ttf/

Este script se ejecutará con todos los parámetros establecidos en la sentencia, que a continuación detallamos:

--with-oci8=/mnt/db	Integra el cliente de la base de datos. Se indica el punto de montaje del cliente oracle
--with-apxs2=/usr/local/apache2/bin/apxs/	Integra el php con el servidor web Apache. Se indica la ruta local de los binarios de Apache
--with-ldap	Se integra el cliente de LDAP
--with-openssl=/usr/local/ssl	Integra al servidor web apache y php el protocolo SSL. Se indica la ruta local del servidor ssl
--with-gd --with-jpeg-dir --with-zlib-dir --with-freetype-dir --with-png-dir --with-xpm-dir --enable-gd-native-ttf/	Se integra todas las librerías gráficas que se utilizaran con php y el servidor web

Tabla 24 Configuración de apache

Una vez realizada la configuración de php, se procede a compilar y luego enlazar todos los archivos necesarios para que funcione php.

Finalmente se procede a verificar realizando algún pequeño script en php para probar la integración del php, apache y la base de datos.

4.9.7 Seguridades de php

Las seguridades en php también deben ser consideradas de manera muy importante como las de apache como servidor web, por ser una herramienta de código abierto, es necesario también mantener actualizado el software, con todos los parches y configuraciones adecuadas de php.

Principalmente en nuestro caso, en que php está integrado como un módulo de Apache, en donde existen riesgos como el que el usuario del servidor web, apache, incluso el usuario “nobody” que es el predeterminado en apache, herede los permisos para php, esto significa que si se tiene acceso a bases de datos, podría ejecutar un código malicioso con sentencias de borrado de los objetos de la base de datos. Para evitar este tipo de inconvenientes, se usa otro usuario para que acceda a la base de datos, e incluso que se conecte a nuestro servidor de contenido mediante NFS donde están alojadas las páginas web y la base de datos. Solo se la da privilegios de lectura, y además negarle al usuario realizar conexiones remotas, o acceso al shell de usuario.

La interacción con la base de datos desde php es también importante en el tema de seguridades, y más aún en aplicaciones web, una norma de seguridad es que siempre se debe abrir la conexión, ejecutar la sentencia

sql, y una vez devueltos los datos desde la base, inmediatamente se debe cerrar la conexión desde php.

En vista que las operaciones que se realizan sobre una base de datos, siempre es necesario tener un usuario con acceso a la base, es importante que ese usuario no sea tan fácil e incluso la contraseña sea compleja, para evitar riesgos de seguridad y de que puedan borrar la base, ya que este usuario muchas veces está embebido en el código de los scripts de php. Por ello también es importante, implementar seguridades a nivel del código de programación en php.

Gracias a la ventaja de que php es un lenguaje que soporta programación orientada a objetos, entonces, se puede realizar protecciones a nivel de código, y de esta manera se está protegiendo la integridad de los datos.

Por lo tanto, siempre se debe mantener actualizado este lenguaje, su configuración y todo lo relacionado a él. De tal manera que se puede evitar posibles ataques de intrusos.

4.9.8 Instalación y configuración de ssl

Para objetivos prácticos de nuestro proyecto, se debió implementar un servidor que emita los certificados de autenticación y validación para las comunicaciones seguras en nuestro servidor web, es decir usando el protocolo SSL. Realmente a nivel del servidor web se debería generar un

certificado ssl, X509, y enviarse a una entidad certificadora, de tal manera que realice la firma digital y nos de la autenticidad de nuestro certificado para ser instalado en nuestro servidor web. Con este se le da al cliente o usuario la veracidad, confidencialidad de que las transmisiones son seguras entre el cliente browser y nuestro servidor web, especialmente en el momento que se realice la autenticación de los usuarios de acceso al sistema de pagos electrónicos en línea.

Para realizar la instalación de un certificado de seguridad procedimos a instalar el software que realice tales tareas, como es el openssl. Que es una aplicación de código abierto, y que es compatible con nuestro sistema operativo Linux. Es más, hoy en día es parte esencial en el sistema operativo.

Escogimos la última versión disponible en el sitio web del software como es www.openssl.org.

Una vez instalado procedimos a generar el respectivo certificado con la siguiente sentencia en el servidor web.

Openssl genrsa –des3 –out srvapp.key 2048

Openssl rsa –in srvapp.key –out srvapp.pem

Openssl req –new –key srvapp.key –out srvapp.csr

Openssl x509 –req –days 365 –in srvapp.csr –signkey srvapp.key –out srvapp.crt

Con estas sentencias se procedió a generar las respectivas claves de nuestro servidor, y luego se generó el certificado y se lo firmó como un certificado X509 compatible con todos los clientes browser que soporten la encriptación del protocolo ssl, para realizar las comunicaciones seguras.

De tal manera que el servidor web ya puede levantar el servicio de http para publicar el sistema de pagos electrónicos usando conexiones https, es decir comunicaciones seguras. Con esto se encripta todo el tráfico que se transmita entre el cliente y el servidor web, usando el certificado X509 válido para este servidor.

4.9.9 Configuración de firewall web

En el servidor web también se ha considerado las seguridades a nivel de host, es decir, que se configuró al firewall del sistema operativo de manera similar que el firewall a nivel de red.

Es decir, que solo está permitido acceder al servicio web, usando el protocolo http y ssl, desde la red externa o Internet, pero a nivel de las redes internas, se debe permitir el acceso hacia el servidor de contenido y el acceso a la base de datos por tal razón, se debe permitir el acceso a los puertos TCP que use el cliente de oracle y el cliente NFS.

Con esto se asegura que sólo se usará estos puertos, mientras que los demás deberán ser bloqueados para evitar posibles fallas de seguridad.

A continuación se detalla las reglas en el firewall del servidor web.

Origen	Destino	Protocolo	Acceso
Servidor web	Servidor contenido	Tcp oracle	Permitido
Servidor contenido	Servidor web	tcp oracle	Permitido
Servidor web	Servidor contenido	Tcp cliente nfs	Permitido
Servidor contenido	Servidor web	Tcp nfs	Permitido
Internet	Servidor web	http	Permitido
Internet	Servidor web	Ssl	Permitido
Servidor web	Internet	http	Permitido
Servidor web	Internet	Ssl	Permitido

Tabla 25 Politica del firewall del servidor web

Cada una de estas reglas deberá ser definida en el firewall del host, que en este caso usamos IPTABLES, para el cual se debe escribir las reglas según la sintaxis que usa este programa que hace la función de firewall.

Con esto mantendremos sólo el tráfico necesario entre las diferentes capas de acceso hacia los servidores requeridos.

CAPITULO V

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN SITIO DE SISTEMA DE PAGO ELECTRÓNICO

5.1 Análisis de un sitio Web de sistema de pago electrónico

5.1.1. Requerimientos Funcionales

De manera general podemos enunciar los siguientes Requerimientos Funcionales de un sitio de pago electrónico:

- Diseñar e implementar un sitio web de sistema pago electrónico.
- Permitir que los clientes del sistema de pago se autentiquen por medio de un usuario y una contraseña.
- Permitir que los clientes del sistema de pago, mantengan una cuenta virtual en el sistema.
- Permitir que los clientes de cuenta en el sitio de pago, puedan consultar sus movimientos en cualquier momento.
- Permitir que los clientes a través de su cuenta virtual puedan enviar o recibir dinero a través del correo electrónico.
- Permitir que los clientes a través de su cuenta virtual, puedan pagar por bienes y/o servicios en sitios de comercio electrónico afiliados al sistema de pago.

- Permitir que los clientes dueños de sitios de comercio electrónico ofrezcan a sus clientes comprar mediante el sistema de pago.
- Permitir que el cliente dueño de la cuenta virtual utilice una tarjeta de crédito o débito a cuenta bancaria para realizar los movimientos reales de dinero.
- Permitir que cualquier usuario pueda navegar por los enlaces informativos del sitio.
- Permitir que cualquier usuario pueda tener una cuenta virtual en el sistema de pago con solo especificar su correo electrónico e información indispensable para el registro.
- Permitir que el cliente del sistema de pago, pueda depositar dinero en su cuenta virtual, especificando su tarjeta de crédito o cuenta bancaria por única ocasión.

5.1.2. Requerimientos No Funcionales

- Implementar el sitio web de sistema de pago, bajo un esquema de autenticación segura.
- Implementar un esquema de red seguro, confiable y protegido de cualquier ataque malicioso interno o externo.
- Trabajar en un esquema de contingencia, de manera que el sitio sea de alta disponibilidad.

- Implementar seguridades en todos los niveles del desarrollo, de manera de ofrecer total integridad en la información. Utilización de encriptación de contraseñas y códigos de sesión.
- Requerimientos de hardware que permitan el rendimiento adecuado hacia el usuario final.

5.1.3. Modelo de Casos de Uso

Casos de Uso

1. Un Usuario se registra como Miembro del Sitio de pago
2. Un Miembro hace un login al sitio de Pago
3. Un Miembro registra una cuenta bancaria a su cuenta del sitio de pago
4. Un Miembro registra una tarjeta de crédito a su cuenta del sitio de pago
5. Un Miembro agrega fondos a la cuenta del sitio de pago
6. Un Miembro realiza un pago en un sitio e-commerce autorizado
7. Un Miembro retira fondos de la cuenta del sitio de pago
8. Un Miembro envía dinero a un correo electrónico
9. Un Miembro consulta movimientos de su cuenta
10. Un Miembro cambia la contraseña de su cuenta
11. Un Miembro olvidó su contraseña de su cuenta
12. Un Miembro cambia información de crédito de la cuenta del sitio de pago
13. Un Miembro cambia la dirección o teléfono de su cuenta

5.1.3.1. Un Usuario se registra como Miembro del Sitio de Pago

Definición: Un usuario quien desea usar los servicios del sitio de pago, debe registrarse como Miembro, creando una cuenta virtual.

Si es una persona natural, debe crear una Cuenta Personal.

Si es una persona jurídica quien posee un sitio de comercio electrónico debe crear una Cuenta Empresarial.

Si el registro es exitoso, el Usuario recibirá un correo con los datos necesarios para registrarse por primera vez y utilizar los servicios de pago.

Requiere el registro de datos personales.

Notas:

- La Membresía es sin costo alguno.
- El Usuario tiene opción de registrarse con Cuenta Personal o Cuenta Empresarial.
- Siempre se debe indicar la dirección de correo electrónico, una contraseña y una pregunta y respuesta secretas.
- Si es una Cuenta Empresarial, se debe indicar el url del sitio de comercio electrónico.

- ❖ Una vez verificada la información, se confirma el registro y se envía una notificación a la dirección de correo registrada, indicando un código PIN y un link a la página de registro por primera vez.
- ❖ La primera vez que se registra deberá ingresar la dirección de correo electrónico, la contraseña y el Código de Seguridad.
- ❖ Si existe alguna validación sin éxito, se da un aviso al Usuario y no se crea la cuenta del sitio de pago.

Actores

- Usuario de Internet
- Sitio de Pago

5.1.3.2. Un Miembro realiza login al sitio

Definición: Un Miembro realiza el login indicando la dirección de correo y su contraseña.
Una vez validada esta información puede acceder al perfil de su cuenta y las opciones de la misma.

Notas

- ❖ Siempre debe indicar la dirección de correo y la contraseña y el Código de Seguridad.
- ❖ Se pueden hacer hasta tres intentos de login, pasado de este número se le indicará que se le enviará un correo a su dirección para una nueva confirmación de datos.
- ❖ Si la información es válida, ingresa al perfil de la cuenta, donde se mostrará el saldo de la misma, los últimos movimientos y las opciones que se pueden realizar.
- ❖ Se debe verificar que la cuenta esté activa y no sea el primer login de una nueva cuenta.
- ❖ Si es el primer login, no podrá ingresar al sitio. El primer login debe hacerse desde el link enviado por correo.

Actores

- Usuario Miembro del Sitio de Pago
- Sitio de Pago

5.1.3.3. Un Miembro registra una cuenta bancaria a su cuenta del sitio de pago

Definición: Un Miembro desea realizar transacciones con su cuenta, para ello registra una cuenta bancaria para relacionarla a todas las transacciones de su cuenta del sitio de pago.

Notas

- Si el Miembro reside en Ecuador, tiene opción a definir la cuenta bancaria de una entidad financiera nacional.
- Si el Miembro reside en el exterior, no puede registrar cuentas bancarias.
- Se verifica que la cuenta exista en la entidad financiera indicada, que esté activa y que pertenezca al titular indicado.
- Si la verificación es exitosa, la información de la cuenta bancaria quedará relacionada para todas las transacciones realizadas con la cuenta del sitio de pago.
- Si la información de crédito es verificada sin éxito, se da un aviso al Usuario y no se crea la cuenta virtual.

Actores

- Usuario de Internet
- Sitio de Pago
- Entidad Financiera Nacional

5.1.3.4. Un Miembro registra una tarjeta de crédito a su cuenta del sitio de pago

Definición: Un Miembro desea realizar transacciones con su cuenta, para ello registra una tarjeta de crédito para relacionarla a todas las transacciones de su cuenta del sitio de pago.

Notas

- Si el Miembro reside en Ecuador o en el exterior, tiene opción a definir una tarjeta de crédito: American Express, Visa Internacional, Mastercard y Diners.
- Se verifica que la cuenta exista en la entidad financiera indicada, que esté activa y que pertenezca al titular indicado.
- Si la verificación es exitosa, la información de la tarjeta de crédito quedará relacionada para todas las transacciones realizadas con la cuenta del sitio de pago.
- Si la información de crédito es verificada sin éxito, se da un aviso al Usuario y no se crea la cuenta del sitio de pago.

Actores

- Usuario de Internet
- Sitio de Pago
- Entidad de Tarjeta de Crédito

5.1.3.5. Un Miembro agrega fondos a su cuenta del sitio de pago

Definición: Un Miembro registrado con Cuenta Personal o Cuenta Empresarial desea depositar dinero en su cuenta del sitio de Pago.

Indicará el monto que desea depositar en la cuenta.

Si es exitoso, el saldo de la cuenta virtual se incrementará por el valor depositado y se envía información de débito a la cuenta bancaria o tarjeta de crédito.

Notas:

- El monto mínimo de depósito, la primera vez es de $ 50.00
- El monto máximo por depósito es de $ 500.00
- Se cobrará un recargo por depósito de 1% sobre el monto del mismo.
- Se verificará el saldo disponible en la cuenta bancaria o el cupo en la tarjeta de crédito para aprobar la transacción.
- Se notificará al Miembro su saldo en la cuenta virtual.

- ❖ Se enviará información de débito a la cuenta bancaria o tarjeta de crédito.
- ❖ Se enviará correo a la cuenta del Miembro notificando la transacción exitosa.

Actores

- Usuario de Internet
- Entidad financiera nacional
- Entidad de Tarjeta de Crédito

5.1.3.6. Un Miembro realiza un pago en sitio e-commerce autorizado

Definición: Un Miembro de Cuenta Personal, realiza un pago por la compra de bienes o servicios en un sitio e-commerce registrado como Miembro de Cuenta Empresarial del sitio de pago.

Si es exitoso, se registrará un débito en la Cuenta Personal del comprador por el monto de la compra, y un crédito en la Cuenta Empresarial del vendedor por el mismo monto.

Notas

- Todo Miembro de Cuenta Empresarial, tiene la opción de colocar en su sitio, un botón con el cual el comprador decide pagar por medio del sitio de pago.
- El comprador debe ser tener una Cuenta Personal en el sitio de pago, indicar la dirección de correo de su cuenta, la contraseña y el Código de Seguridad indicado en la transacción.
- Si el comprador tiene saldo suficiente en su Cuenta Personal del sitio de pago que cubra la transacción, se confirma que la transacción fue exitosa.
- Si la transacción fue exitosa, se registra un débito en la Cuenta Personal del comprador y un crédito en la Cuenta Empresarial del vendedor.
- Esta transacción no tiene recargo alguno para el comprador.
- Si el comprador no tiene saldo suficiente en su Cuenta Personal, se confirma que la transacción fue cancelada.
- Tanto el Comprador como el Vendedor recibirán notificaciones de las transacciones realizadas en las cuentas respectivas.

Actores

- Usuario Comprador de Internet
- Sitio de Comercio electrónico o Vendedor.

- Entidad financiera nacional
- Entidad de Tarjeta de Crédito

5.1.3.7. Un Miembro retira fondos de la cuenta del sitio de pago

Definición: Un Miembro del sitio de pago retira fondos de la cuenta.

Notas

- ❖ Por cada retiro el sitio de pago cobra 1 dólar, sin importar el monto del mismo.
- ❖ Se verifica que el saldo en la cuenta sea mayor o igual al monto de retiro más el recargo.
- ❖ Se registra un débito en la cuenta virtual por el monto de retiro y por el recargo y un crédito en la cuenta bancaria o tarjeta de crédito por el monto de retiro.
- ❖ El Miembro recibirá notificación de correo de la transacción realizada.

Actores

- Usuario Miembro del Sitio de Pago
- Entidad financiera nacional

- Entidad de Tarjeta de Crédito

5.1.3.8. Un Miembro envía dinero a un correo electrónico

Definición: Un Miembro envía dinero por medio de su cuenta del sitio de pago, indicando el correo electrónico del Destinatario o Beneficiario.

Notas

- ❖ El envío de dinero no tiene ningún costo adicional.
- ❖ Se debe indicar el monto de dinero que se desea enviar, el nombre del Beneficiario y el correo electrónico del Beneficiario.
- ❖ Si el Miembro tiene saldo en su cuenta que cubre el movimiento de dinero, se realiza el débito por el monto especificado.
- ❖ Se enviarán notificaciones al Miembro y al Beneficiario.
- ❖ Si el Beneficiario no tiene cuenta en el sitio de pago, debe registrarse para poder obtener el envío de dinero.

Actores

- Miembro del sitio de pago
- Beneficiario del envío

- Sitio de Pago

5.1.3.9. Un Miembro consulta movimientos de su cuenta

Definición: Un Miembro desea consultar los movimientos en su cuenta virtual. Puede indicar un rango de fechas y el tipo de transacción.

Notas

- ❖ El Miembro debe indicar la fecha inicial y fecha final de búsqueda y el tipo de transacción: débitos, créditos o todas.
- ❖ Se presentará la información solicitada indicando: fecha de la transacción, tipo de transacción, monto de la transacción, si es un pago el nombre del sitio y la dirección de correo del vendedor.
- ❖ Se mostrará un saldo inicial y un saldo final.

Actores

- Usuario Miembro del Sitio de Pago
- Entidad financiera nacional
- Entidad de Tarjeta de Crédito

5.1.3.10. Un Miembro cambia la contraseña de su cuenta

Definición: Un miembro desea cambiar la contraseña de su Cuenta.

Se solicitará que confirme la respuesta a la pregunta secreta indicada en el registro de la cuenta.

Si la respuesta es positiva, se permitirá la definición de una nueva contraseña.

Notas

- En el registro de la cuenta virtual, se solicita definir una contraseña y confirmar la misma, a su vez se debe indicar una pregunta secreta y la respuesta a la misma.
- Cuando el Miembro desea cambiar su contraseña, se solicita que se indique: la dirección de correo y un Código de Seguridad. Si la información es válida, se solicita contestar la pregunta secreta. Si la respuesta es válida, se permite indicar una nueva contraseña y confirmar la misma.
- El Miembro recibirá notificación en su correo del cambio realizado.

Actores

- Usuario Miembro del Sitio de Pago
- Entidad financiera nacional
- Entidad de Tarjeta de Crédito

5.1.3.11. Un Miembro olvidó la contraseña de su cuenta

Definición: Un miembro olvidó la contraseña de su Cuenta.

Se solicitará que confirme la respuesta a la pregunta secreta indicada en el registro de la cuenta.

Si la respuesta es positiva, se permitirá la definición de una nueva contraseña.

Notas

- ❖ En el registro de la cuenta virtual, se solicita definir una contraseña y confirmar la misma, a su vez se debe indicar una pregunta secreta y la respuesta a la misma.
- ❖ Cuando el Miembro olvidó su contraseña, se solicita que se indique: la dirección de correo y un Código de Seguridad. Si la información es válida,

se solicita contestar la pregunta secreta. Si la respuesta es válida, se permite indicar una nueva contraseña y confirmar la misma.

- ❖ El Miembro recibirá notificación en su correo del cambio realizado.

Actores

- Usuario Miembro del Sitio de Pago
- Entidad financiera nacional
- Entidad de Tarjeta de Crédito

5.1.3.12. Un Miembro cambia información de crédito de la cuenta del sitio de pago

Definición: Un Miembro desea cambiar la cuenta bancaria o tarjeta de crédito indicada en el registro de la cuenta. Se verificará la nueva información de crédito.

Notas

- ❖ Si el Miembro reside en Ecuador, puede definir una cuenta bancaria de entidades financieras locales o tarjeta de crédito.
- ❖ Si el Miembro reside en el exterior, solo puede definir tarjeta de crédito.
- ❖ Se verificará la nueva información de crédito.
- ❖ Si la verificación es positiva, se confirma el cambio y se lleva un registro del mismo.
- ❖ Si la verificación es negativa, se informa al Miembro que el cambio fue cancelado.
- ❖ El Miembro recibirá notificación a su correo del cambio realizado.

Actores

- Usuario Miembro del Sitio de Pago
- Entidad financiera nacional
- Entidad de Tarjeta de Crédito

5.1.3.13. Un Miembro cambia la dirección o teléfono de su cuenta

Definición: Un Miembro desea actualizar la dirección o teléfono registrados en su cuenta del sitio de pago.

Notas

- ❖ Debe actualizarse la dirección que conste en la Tarjeta de Crédito, si esa será la cuenta relacionada, de manera que se pueda verificar cualquier transacción.
- ❖ Cualquier actualización realizada se notificará al correo electrónico.

Actores

- Usuario Miembro del Sitio de Pago
- Sitio de Pago

5.1.4. Escenarios

Caso de Uso 1: Un Usuario se registra como Miembro del Sitio de Pago

Escenario 1.1: Registro de Cuenta Personal (exitoso)

Supuestos:

- El Usuario posee cuenta de correo electrónico válida.

- El Usuario es una persona natural que reside en Ecuador o en el exterior.
- Ingresa datos personales, contraseña y código de sesión correctamente.

Salidas

- Se confirma la creación de la cuenta personal.
- Se envía notificación al correo electrónico indicado en el registro para confirmar la validez del mismo y pueda realizar el primer login a la cuenta.

Escenario 1.2: Registro de Cuenta Personal (sin éxito)

Supuestos

- El Usuario es una persona natural que reside en Ecuador.
- El Usuario posee una cuenta de correo electrónico válida.
- No se cumplen todas las validaciones de datos personales, o contraseña o código de sesión.

Salidas

- Se notifica al Usuario el problema en la validación.

- No se crea la cuenta.

Escenario 1.3: Registro de Cuenta Empresarial (exitoso)

Supuestos

- El Usuario es una persona jurídica legalmente constituida que reside en Ecuador o en el exterior.
- El Usuario posee una cuenta de correo electrónico válida.
- El Usuario posee un sitio de comercio electrónico verificado.
- Se confirma la validez de todos los datos ingresados: información de la empresa, contraseña, código de sesión.

Salidas

- Se confirma la creación de la cuenta Empresarial
- Se envía notificación al correo electrónico indicado en el registro para confirmar la validez del mismo y pueda realizar el primer login a la cuenta.

Escenario 1.4: Registro de Cuenta Empresarial (sin éxito)

Supuestos

- El Usuario es una persona jurídica legalmente constituida que reside en Ecuador o en el exterior.
- El Usuario posee una cuenta de correo electrónico válida.
- El Usuario posee un sitio de comercio electrónico verificado.
- Se confirma la invalidez de alguno de los datos ingresados: información de la empresa, contraseña, código de sesión.

Salidas

- Se notifica al Usuario el problema en la validación.
- No se crea la cuenta.

Caso de Uso 2: Un Miembro hace un login al sitio de pago

Escenario 2.1: Login exitoso

Supuestos

- Cuenta de correo registrada

- Contraseña correcta
- Código de sesión ingresado correctamente.

Salida

- Permitir acceso a cuenta de sitio de pago

Escenario 2.2: Login sin éxito (cuenta no registrada)

Supuestos

- Cuenta no registrada

Salidas

- Se notifica al Usuario que no se encuentra registrado el Correo indicado.
- No se permite el acceso a la cuenta virtual

Escenario 2.3: Login sin éxito (contraseña incorrecta)

Supuestos

- Cuenta registrada
- Contraseña incorrecta

Salidas

- Se notifica al usuario la invalidez de la contraseña.
- No se permite el acceso a la cuenta virtual

Escenario 2.4: Login sin éxito (contraseña incorrecta tercer intento)

Supuestos

- Cuenta registrada
- Contraseña incorrecta
- Tercer intento de login sin éxito

Salidas

- No se permite el acceso a la cuenta virtual
- Se envía correo electrónico para confirmación de datos y login seguro
- Se bloquea el acceso hasta confirmar login por link enviado por correo.

Caso de Uso 3: Un Miembro registra una cuenta bancaria a su cuenta del sitio de pago

Escenario 3.1: Registro de cuenta bancaria válida

Supuestos

- El Usuario posee una cuenta bancaria activa en la entidad financiera local indicada.
- El Usuario posee una cuenta de correo electrónico válida.

Salidas

- Se confirma la validez de la cuenta bancaria
- Se registra la cuenta.

Escenario 3.2: Registro de Cuenta con cuenta bancaria (sin éxito)

Supuestos

- La información de cuenta bancaria no es válida: la cuenta no existe, la cuenta está cerrada, nombre de titular incorrecto, tipo de cuenta incorrecto.

Salidas

- Se confirma la invalidez de la cuenta bancaria.
- No se registra la cuenta.

Caso de Uso 4: Un Miembro registra una tarjeta de crédito a su cuenta del sitio de pago

Escenario 4.1: Registro de tarjeta de crédito válida

Supuestos

- El Usuario posee una tarjeta de crédito internacional válida.

Salidas

- Se confirma la validez de la tarjeta de crédito.
- Se registra la tarjeta.

Escenario 4.2: Registro de tarjeta de crédito inválida

Supuestos

- El Usuario posee una tarjeta de crédito internacional no válida: la fecha de expiración está vencida, el número de tarjeta no existe, el nombre del titular incorrecto.

Salidas

- Se confirma la invalidez de la tarjeta.
- No se registra la tarjeta.

Caso de Uso 5: Un Miembro agrega fondos a la cuenta del sitio de pago

Escenario 5.1: Agregar fondos de tarjeta de crédito (exitoso)

Supuestos

- La tarjeta de crédito no está vencida y tiene cupo ilimitado.

Salidas

- Se registra un crédito a la cuenta virtual por el monto especificado.
- Se registra un débito a la tarjeta de crédito por el monto especificado más el recargo.
- Se incrementa el saldo disponible.

Escenario 5.2: Agregar fondos de cuenta bancaria (exitoso)

Supuestos

- La cuenta bancaria está activa.
- Saldo de la cuenta bancaria suficiente.

Salidas

- Se registra un crédito a la cuenta virtual por el monto especificado.
- Se registra un débito a la cuenta bancaria por el monto especificado más el recargo.

- Se incrementa el saldo disponible de la cuenta virtual.

Escenario 5.3: Agregar fondos de tarjeta de crédito (sin éxito)

Supuestos

- La tarjeta de crédito no es válida: fecha vencida o cupo insuficiente.

Salidas

- Se informa de cancelación de transacción.
- No se realiza transacción.

Escenario 5.4: Agregar fondos de cuenta bancaria (sin éxito)

Supuestos

- La cuenta bancaria no es válida: cerrada o saldo insuficiente.

Salidas

- Se informa de cancelación de transacción.

- No se realiza transacción.

Caso de Uso 6: Un miembro realiza pago en un sitio e-commerce autorizado

Escenario 6.1: Realiza pago exitoso

Supuestos

- User y contraseña válidos
- Saldo en cuenta virtual suficiente
- Monto máximo no excedido

Salidas

- Confirmación de pago realizado
- Se registra un débito en la cuenta del comprador.
- Se registra un crédito en la cuenta del vendedor.
- Se envían notificaciones a ambas cuentas.

Escenario 6.2: Realiza pago sin éxito (user incorrecto)

Supuestos

- User no válido. Cuenta inexistente.

Salidas

- Confirmación de pago sin éxito.
- No se realiza ninguna transacción.
- Se notifica a la cuenta del vendedor, la cancelación de la transacción.

Escenario 6.3: Realiza pago sin éxito (contraseña incorrecta)

Supuestos

- Contraseña incorrecta.

Salidas

- Confirmación de pago sin éxito.
- No se realiza ninguna transacción.
- Se notifica a la cuenta del vendedor, la cancelación de la transacción.

Escenario 6.4: Realiza pago sin éxito (saldo insuficiente)

Supuestos

- User y contraseña válidos.
- Saldo en cuenta virtual de comprador insuficiente.
- Monto máximo no excedido

Salidas

- Confirmación de pago sin éxito.
- No se realiza ninguna transacción.
- Se notifica a la cuenta del vendedor, la cancelación de la transacción.

Escenario 6.5: Realiza pago sin éxito (monto excedido primera vez)

Supuestos

- User y contraseña válidos.
- Saldo en cuenta virtual de comprador suficiente.
- Monto máximo de transacción excedido

Salidas

- Confirmación de pago sin éxito.
- No se realiza ninguna transacción.
- Se notifica a la cuenta del vendedor, la cancelación de la transacción.
- Se notifica a la cuenta del comprador que se cancela la transacción por exceder el monto máximo por transacción.

Escenario 6.6: Realiza pago sin éxito (monto excedido segunda vez)

Supuestos

- User y contraseña válidos.
- Saldo en cuenta virtual de comprador suficiente.
- Monto máximo de transacción excedido por segunda ocasión

Salidas

- Confirmación de pago sin éxito.
- No se realiza ninguna transacción.
- Se notifica a la cuenta del vendedor, la cancelación de la transacción.

- Se desactiva la cuenta del comprador.
- Se notifica a la cuenta del comprador que se cancela la transacción por exceder el monto máximo por transacción por segunda ocasión y se informa la desactivación de la cuenta.

Caso de Uso 7: Un Miembro retira fondos de la cuenta del sitio de pago

Escenario 7.1: Retiro de fondos a tarjeta de crédito (exitoso)

Supuestos:

- Tarjeta de crédito no vencida.
- Saldo de cuenta virtual suficiente.
- Monto máximo de transacción no excedido
- Número máximo de retiros no excedido.

Salidas

- Se registra un débito en la cuenta virtual por el monto retirado.
- Se registra un crédito en la tarjeta de crédito por el monto retirado deducido el valor de recargo.
- Se decrementa el saldo disponible de la cuenta virtual.

Escenario 7.2: Retiro de fondos a cuenta bancaria (exitoso)

Supuestos:

- Cuenta bancaria activa.
- Saldo de cuenta virtual suficiente.
- Monto máximo de transacción no excedido
- Número máximo de retiros no excedido.

Salidas

- Se registra un débito en la cuenta virtual por el monto retirado.
- Se registra un crédito en la cuenta bancaria por el monto retirado deducido el valor de recargo.
- Se decrementa el saldo disponible de la cuenta virtual.

Escenario 7.3: Retiro de fondos a tarjeta de crédito (sin éxito)

Supuestos:

- Tarjeta de crédito expirada.

Salidas

- Se confirma la invalidez de la tarjeta.
- No se realiza la transacción.

Escenario 7.4: Retiro de fondos sin éxito (cuenta cerrada)

Supuestos:

- Cuenta bancaria cerrada.

Salidas

- Se confirma la invalidez de la cuenta.
- No se realiza la transacción.

Escenario 7.5: Retiro de fondos sin éxito (saldo insuficiente)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual insuficiente

Salidas

- Se confirma la insuficiencia de fondos.
- No se realiza la transacción.

Escenario 7.6: Retiro de fondos sin éxito (monto máximo excedido primera vez)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual suficiente
- Monto máximo por transacción excedido por primera vez

Salidas

- Se confirma la cancelación de la transacción.
- No se realiza la transacción.
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el monto máximo por transacción permitido.

Escenario 7.7: Retiro de fondos sin éxito (monto máximo excedido segunda vez)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual suficiente
- Monto máximo por transacción excedido por segunda vez

Salidas

- Se confirma la cancelación de la transacción.
- No se realiza la transacción.
- Se desactiva la cuenta del cliente.
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el monto máximo por transacción permitido y la desactivación de la cuenta.

Escenario 7.8: Retiro de fondos sin éxito (número de retiros máximo excedido primera vez)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual suficiente
- Monto máximo por transacción no excedido
- Número de retiros máximo excedido por primera vez

Salidas

- Se confirma la cancelación de la transacción.
- No se realiza la transacción.
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el número máximo de retiros por día permitido.

Escenario 7.9: Retiro de fondos sin éxito (número de retiros máximo excedido segunda vez)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual suficiente
- Monto máximo por transacción no excedido
- Número de retiros máximo excedido por segunda vez

Salidas

- Se confirma la cancelación de la transacción.
- No se realiza la transacción.
- Se desactiva la cuenta del cliente.
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el número máximo de retiros por día permitido y se informa la desactivación de la cuenta.

Caso de Uso 8: Un Miembro envía dinero a un correo electrónico

Escenario 8.1: Envío de dinero (exitoso)

Supuestos

- Saldo suficiente en cuenta de sitio de pago
- Correo electrónico del Beneficiario es válido
- Monto máximo de transacción no excedido
- Número máximo de retiros no excedido.

Salidas

- Se confirma la transacción exitosa
- Se envía notificación del débito a la cuenta del Miembro
- Se notifica el envío de dinero al correo del Beneficiario.

Escenario 8.2: Envío de dinero sin éxito (saldo insuficiente)

Supuestos

- Correo electrónico del Beneficiario es válido
- Saldo insuficiente en cuenta del sitio de pago.

Salidas

- Se confirma que la transacción no fue realizada

Escenario 8.3: Envío de dinero sin éxito (correo inválido)

Supuestos

- Correo electrónico del Beneficiario es inválido

Salidas

- Se confirma la invalidez de los datos
- La transacción no se realiza

Escenario 8.4: Envío de dinero sin éxito (monto máximo excedido primera vez)

Supuestos

- Saldo suficiente en cuenta de sitio de pago
- Correo electrónico del Beneficiario es válido
- Monto máximo de transacción excedido por primera vez

Salidas

- Se confirma la cancelación de la transacción
- La transacción no se realiza
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el monto máximo de transacción permitido.

Escenario 8.5: Envío de dinero sin éxito (monto máximo excedido segunda vez)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual suficiente
- Monto máximo por transacción excedido por segunda vez

Salidas

- Se confirma la cancelación de la transacción.
- No se realiza la transacción.
- Se desactiva la cuenta del cliente.

- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el monto máximo de transacción permitido y se informa la desactivación de la cuenta.

Escenario 8.6: Envío de dinero sin éxito (número máximo de retiros excedido primera vez)

Supuestos

- Saldo suficiente en cuenta de sitio de pago
- Correo electrónico del Beneficiario es válido
- Monto máximo de transacción no excedido
- Número máximo de retiros excedido por primera vez

Salidas

- Se confirma la cancelación de la transacción
- La transacción no se realiza
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el número máximo de retiros permitidos al día.

Escenario 8.7: Envío de dinero sin éxito (número máximo de retiros excedido segunda vez)

Supuestos:

- Tarjeta de crédito o cuenta bancaria válida.
- Saldo en cuenta virtual suficiente
- Monto máximo por transacción no excedido
- Número de retiros máximo excedido por segunda vez

Salidas

- Se confirma la cancelación de la transacción.
- No se realiza la transacción.
- Se desactiva la cuenta del cliente.
- Se notifica a la cuenta del cliente que se cancela la transacción por exceder el número máximo de retiros permitidos al día y se informa la desactivación de la cuenta.

Caso de Uso 9: Un Miembro consulta movimientos de su cuenta

Escenario 9.1: Consulta de movimientos (con movimientos)

Supuestos

- Cuenta virtual con movimientos dentro de los parámetros indicados

Salidas

- Movimientos realizados

Escenario 9.2: Consulta de movimientos (sin movimientos)

Supuestos

- Cuenta virtual sin movimientos dentro de los parámetros indicados

Salidas

- Confirmación de que no hay movimientos.

Caso de Uso 10: Un Miembro cambia la contraseña de su cuenta

Escenario 10.1: Cambio de contraseña válido

Supuestos

- Cuenta de correo registrada
- Contraseña actual válida

- Respuesta a pregunta secreta correcta

Salidas

- Cambio de contraseña

Escenario 10.2: Cambio de contraseña sin éxito (contraseña incorrecta)

Supuestos

- Cuenta de correo registrada
- Contraseña actual incorrecta

Salidas

- No se cambia contraseña

Escenario 10.3: Cambio de contraseña sin éxito (cuenta de correo no existe)

Supuestos

- Olvidé la contraseña.

- Cuenta de correo no registrada

Salidas

- No se cambia contraseña

Escenario 10.4: Cambio de contraseña sin éxito (respuesta secreta incorrecta)

Supuestos

- Cuenta de correo registrada.
- Contraseña actual correcta.
- Respuesta secreta incorrecta

Salidas

- No se cambia contraseña

Caso de Uso 11: Un Miembro olvidó su contraseña de su cuenta

Escenario 11.1: Confirmación de contraseña con éxito

Supuestos

- Cuenta de correo indicada está registrada
- Respuesta secreta correcta

Salidas

- Se confirma la contraseña

Escenario 11.2: Confirmación de contraseña sin éxito (cuenta inválida)

Supuestos

- Cuenta de correo indicada no está registrada

Salidas

- No se confirma la contraseña

Escenario 11.3: Confirmación de contraseña sin éxito (respuesta incorrecta)

Supuestos

- Cuenta de correo indicada está registrada
- Respuesta secreta incorrecta

Salidas

- No se confirma la contraseña

Caso de Uso 12: Un miembro cambia información de crédito

Escenario 12.1: Cambio a tarjeta de crédito (exitosa)

Supuestos:

- Los datos de la tarjeta son válidos: número existente, nombre del titular correcto y fecha no vencida.

Salidas

- Se cambian los datos de crédito.

- Se confirma la actualización de los datos
- Se envía notificación al correo electrónico de la actualización realizada.

Escenario 12.2: Cambio a cuenta bancaria (exitosa)

Supuestos

- Miembro reside en Ecuador.
- Cuenta bancaria válida: cuenta existente y activa.

Salidas

- Se realiza la actualización de datos en la cuenta
- Se confirma la actualización
- Se notifica al correo electrónico la actualización realizada

Escenario 12.3: Cambio a tarjeta de crédito sin éxito

Supuestos

- Tarjeta de crédito no válida: la fecha de expiración está vencida, el número de tarjeta no existe, el nombre del titular incorrecto.

Salidas

- Se confirma la invalidez de la tarjeta.
- No se realiza el cambio.

Escenario 12.4: Cambio a Cuenta con cuenta bancaria (sin éxito)

Supuestos

- La información de cuenta bancaria no es válida: la cuenta no existe, la cuenta está cerrada, nombre de titular incorrecto, tipo de cuenta incorrecto.

Salidas

- Se confirma la invalidez de la cuenta bancaria.
- No se realiza el cambio.

Caso de Uso 13: Un Miembro cambia la dirección o teléfono de su cuenta

Escenario 13.1: Cambio de datos con éxito

Supuestos

- Se indican datos nuevos de dirección o teléfono correctos.

Salidas

- Se realiza la actualización de datos en la cuenta
- Se confirma la actualización
- Se notifica al correo electrónico la actualización realizada

Escenario 13.2: Cambio de datos sin éxito

Supuestos

- No se indican los nuevos datos a actualizar

Salidas

- Se confirma la invalidez
- No se realiza actualización

5.2. Diseño de un sitio web de sistema de pago electrónico

5.2.1. Diseño del Diagrama de Entidad Relación

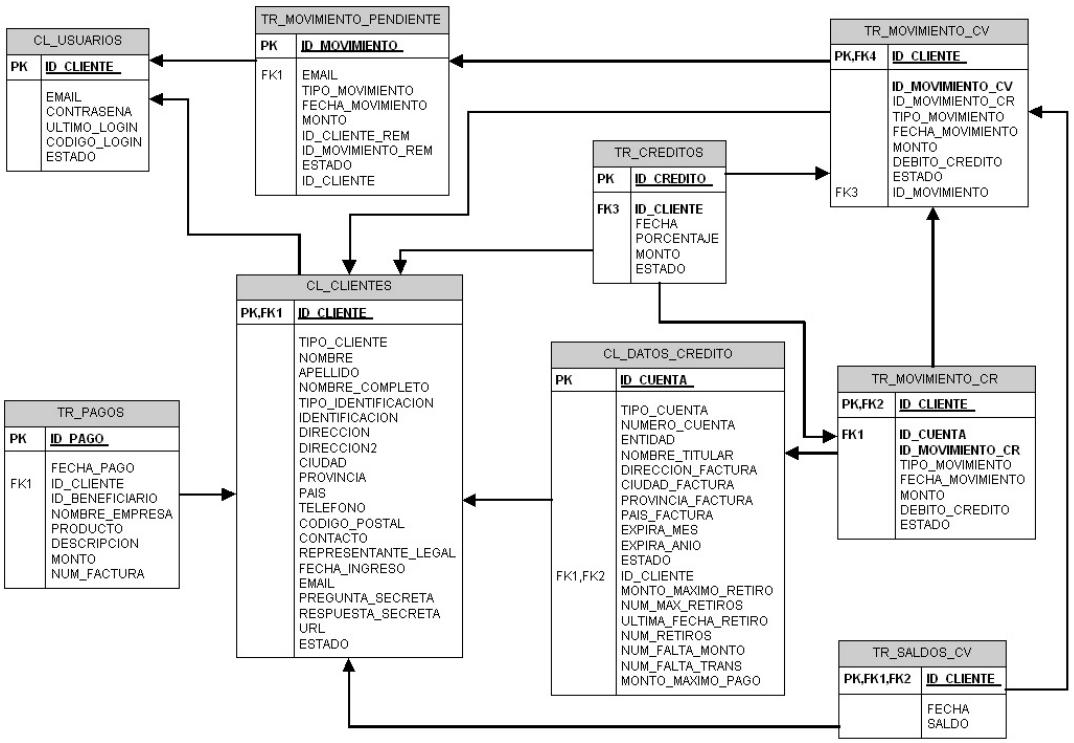


Figura 7 Diagrama Entidad-Relación

5.2.1.1. Entidades

Cl_usuarios.

En esta entidad se lleva la administración de todos los usuarios que se registran en el sistema de pago. Se mantiene la información de: correo electrónico, contraseña encriptada, la fecha y hora del último login y un estado que indica si el usuario confirmó su registro o no.

Cuando el usuario ha confirmado su registro, el sistema permite que pueda ingresar al sistema de lo contrario quedará registrado como Usuario pero no como Cliente.

Cl_clientes.

En esta entidad se administra toda la información del cliente, sea natural o jurídico.

Se guarda información general como: Nombre o representante legal, dirección, ciudad, provincia, país, teléfono, código postal, identificación, pregunta y respuesta secreta, url, fecha de ingreso, etc.

Cl_datos_credito.

En esta entidad se guarda la información relacionada al tipo de cuenta real que manejará el cliente: tarjeta de crédito o cuenta bancaria.

Dependiendo de que se haya elegido se registrará la información sensible necesaria para validarla con los servidores de la institución financiera que corresponda.

Tr_movimiento_cv

En esta entidad se registran todos los movimientos realizados con una cuenta virtual específica. Se lleva un registro del cliente, fecha del movimiento, tipo de movimiento y monto.

Tr_movimiento_cr

Es esta entidad se registran todos los movimientos que se afectarán en la cuenta real relacionada al cliente, sea ésta tarjeta de crédito o cuenta bancaria.

Se lleva un registro del cliente, fecha del movimiento, tipo de movimiento y monto.

Tr_movimiento_pendiente

Cuando un cliente realiza envío de dinero a una cuenta de correo y ésta no está registrada como cuenta del sistema de pago, se crea un registro en esta entidad con el movimiento pendiente para que se active cuando el beneficiario reciba la notificación a su correo electrónico y se registre como usuario de PagoSeguro.

Tr_creditos.

En esta entidad se lleva el registro de los créditos o comisiones que recibe el sistema de pago por cada movimiento en cada cuenta virtual.

Los movimientos que generan comisiones son: Depósitos de dinero, Retiros de dinero y recepción de pagos.

Tr_pagos

En esta entidad se lleva el registro de los pagos realizados a sitios de comercio electrónico por medio del servicio del sistema de pago.

De esta manera se puede notificar tanto al cliente como al establecimiento la información de la transacción realizada como: fecha de pago, nombre de la empresa, producto o bien, descripción del servicio, número de orden o factura de compra y monto de la transacción.

Tr_saldos_cv

En esta entidad se lleva el registro del saldo de cada cuenta virtual de todos los clientes del sistema de pago.

Cada movimiento que se realiza automáticamente actualiza el saldo de la cuenta.

Si_tarjetas_credito

En esta entidad se tiene información para simular el funcionamiento de los servidores operadoras de las tarjetas de crédito.

Si_cuenta_bancaria

En esta entidad se tiene información para simular el funcionamiento de los servidores de instituciones financieras de cuentas bancarias.

5.2.1.2. Procedimientos almacenados

Por seguridad, se desarrollaron los siguientes procedimientos y funciones almacenados en la base de datos:

Cl_crear_cliente

Este procedimiento crea un Cliente en las entidades relacionadas, con la información especificada en el formulario de Registro de Cuenta Personal/Empresarial.

Cl_crear_cuenta

Este procedimiento crea una Cuenta Virtual relacionada al Cliente registrado, pero se especifica la información del formulario de Registro de Tarjeta de Crédito/Cuenta Bancaria.

Cl_existe_cuenta

Por medio de esta función se verifica si el cliente ya ha registrado o no la información de la Cuenta real: tarjeta de crédito o cuenta bancaria.

Cl_verifica_credito

Este procedimiento verifica que la información ingresada en el Registro de Tarjeta de Crédito/Cuenta bancaria, sea validada contra la información de simulación que se tiene de tarjetas de crédito o cuentas bancarias.

Tr_agregar_fondos

Este procedimiento realiza todo el proceso de agregar o ingresar fondos en la cuenta.

Tr_enviar_dinero

Este procedimiento realiza todo el proceso de Enviar dinero a una dirección de correo.

Tr_pagar_compra

Este procedimiento registra toda la transacción de pago de bienes o servicios a través de un sitio de comercio electrónico afiliado al sistema de pago.

Tr_retirar_fondos

Este procedimiento realiza todo el proceso de Retirar dinero de la cuenta virtual y sus transacciones en las otras entidades relacionadas.

Tr_saldo_actual

Esta función devuelve el saldo actual de la cuenta virtual de un cliente específico a una fecha dada.

Tr_verificar_pendiente

Con este procedimiento se verifica al ingresar un nuevo cliente al sistema de pago, de que tenga o no movimientos pendientes de recepción de dinero, para realizar las transacciones necesarias de crédito a su cuenta virtual.

5.3. Tecnologías de desarrollo para sistemas de pago electrónico

5.3.1. PHP

PHP es un acrónimo de Hypertext Preprocessor. Es un lenguaje de programación de código abierto de alto nivel, embebido en páginas HTML y que se ejecuta en el servidor web, a diferencia de otros códigos que se ejecutan en el cliente.

PHP puede ser utilizado en cualquiera de los principales sistemas operativos del mercado, incluyendo Linux, muchas variantes de Unix, Microsoft Windows, Mac OS, etc.

PHP soporta la mayoría de servidores web de hoy en día, incluyendo Apache, Microsoft Internet Information Server, Personal Web Server, Netscape y muchos otros

PHP tiene módulos disponibles para la mayoría de servidores, para aquellos otros que soporten el estándar CGI, PHP puede usarse como procesador CGI.

También tiene la posibilidad de usar programación procedimental o programación orientada a objetos.

Con PHP no se encuentra limitado en cuanto a resultados en HTML. Entre las habilidades de PHP se incluyen: creación de imágenes, archivos PDF y películas flash sobre la marcha. También puede presentar otros resultados como XHTM y archivos XML.

Quizá la característica más destacable de PHP es su soporte para una gran cantidad de bases de datos: Oracle, SQL, mySQL, dBase, IBM DB2, Informix, Sybase, ODBC, Adabas D, Empress, FilePro, Hyperwave, Ingres, InterBase, FronBase, Ovrimos, PostgreSQL, Solid, Velocis, Unix dbm.

También cuenta con soporte para comunicarse con otros servicios usando protocolos tales como LDAP, IMAP, SNMP, NNTP, POP3, HTTP, COM y muchos otros.

Por todas estas facilidades y funcionalidades, se ha escogido este lenguaje para implementar el sitio web de sistema de pago electrónico.

5.3.2. ASP.NET

Es un completo marco de trabajo de construcción de aplicaciones Web. Una de las principales características de este modelo es la flexibilidad de escoger su lenguaje de programación.
Trabaja con lenguajes de script como VBScript, JScript, Perlscript y Pitón, así como lenguajes compilados como VB, C, Cobol, Smalltalk y Lisp.

También proporciona una programación orientada a objetos, herencias, polimorfismos y encapsulación son soportados.

Del lado de la metodología y el lenguaje de programación, el acceso a la base de datos es un tema significante. Cuando un programa ASP.NET, se integra con la base de datos se logra a través de ODBC, el cual proporciona un conjunto consistente de funciones para acceder a su base de datos.

La principal fortaleza es su limpio diseño e implementación, flexibilidad en el lenguaje y sofisticadas características de soporte orientado a objetos. También, presenta un ambiente de sofisticado de depuración de errores.

Pero presenta costos en eficiencia, es muy costoso en el uso de memoria y en tiempo de ejecución. Para aplicaciones basadas en web, estas limitaciones pueden llegar a ser un serio problema.

También presenta un reto en seguridad, ya que exige el uso de Internet Information Server, y este tiene una larga historia de vulnerabilidades.

5.4. Implementación de un sitio web de sistema de pago electrónico

5.4.1. Arquitectura de Capas

El sistema de pago PagoSeguro.com se implementó con una arquitectura Cliente/Servidor, utilizando las siguientes capas:

- Browser cliente
- Web Server
- Application Server
- Database Server

Browser cliente

Recibe de la página HTML, la información de usuario (correo electrónico) y contraseña para autenticar el ingreso y permitir el acceso al sistema.

Web Server

Es el encargado de atender los pedidos de los browser clientes.

Realizará las validaciones necesarias de la información que el cliente ingrese en los formularios, y devolverá respuesta al usuario.

Si las transacciones son exitosas o no, le comunicará al cliente y enviará correos de confirmación.

En este servidor se utilizó Apache Web Server 2.0

Como lenguaje de programación para implementar la lógica y el manejo de las páginas HTML, se utilizó PHP.

Application Server

Se encuentra conectado a los operadores de tarjetas de crédito a través de un enlace dedicado con protocolo TCP/IP.

Se comunica a través de una red privada con el Web Server. Recibe las transacciones del Web Server y realiza la comunicación con los servidores de tarjetas de crédito para validar la información sensible.

Este servidor se implementaría en conjunto cuando se establezca la relación con la institución o entidad financiera que corresponda.

Database Server

En el se guarda la información de usuarios y contraseñas (encriptación). También tiene registrando los movimientos realizados con las cuentas virtuales.

En el servidor de base de datos, se utilizó Oracle 9i Entreprise Edition Release 2.

5.4.2. Por qué Oracle?

Oracle es una poderosa base de datos para construir aplicaciones basadas en web.

Una de las principales características que la denotan por sobre los otros motores, es la seguridad. Por medio de las definiciones de usuarios, privilegios, roles y perfiles se puede administrar los recursos de la base con mayor seguridad.

En el desarrollo de la aplicación utilizamos Oracle 9i Release 2, que mantiene soporte sobre Apache web Server y PHP.

Además, dentro de las nuevas capacidades que trae Oracle 9i, se encuentran las siguientes:

- Autenticación basada en certificados con autenticación basada en password para usuarios empresariales
- No habría necesidad de utilizar SSL.
- Uso de credenciales almacenadas en un directorio LDAP.
- Administración de llaveros, con encriptación más fuerte utilizando algoritmo triple-des.

5.4.3. Por qué PHP?

Se eligió PHP sobre Active Server Pages y JSP como nuestro lenguaje de programación del lado del servidor web, por su velocidad, beneficios de costos, librerías extensivas y su personalización comparada con otras tecnologías web. Usando PHP también nos liberamos de estar atados a un proveedor particular de herramientas de desarrollo. El soporte está disponible en el web a través de una red de sitios y forums de programadores que proporcionan tips útiles en problemas avanzados. Algunos sitios ofrecen una gran variedad de código que pueden ser usados para desarrollar componentes de una gran aplicación.

Además que ofrece soporte sobre la gran mayoría de plataformas de sistemas operativos y motores de bases de datos, sin necesidad de tener conocimientos muy avanzadas para cada plataforma.

También un factor decisivo, fue que al diseñar nuestra base de datos en Oracle, Oracle ha escogido a PHP como la tecnología indicada para desarrollar sus productos en la web.

Y en el aspecto de seguridad, PHP trabaja sobre Apache web Server, lo que facilita el poder implementar las seguridades del caso, que si se tendría que trabajar sobre otra tecnología de web Server.

Podemos mencionar las siguientes ventajas que ofrece:

- Precio. Por ser de código abierto es gratis, pero de todas formas hay que considerar los costos de implementación, mantenimiento y prueba, pero aún es menos costoso que otra tecnología
- Velocidad y eficiencia. Ofrece la ventaja de realizar programas con menos codificación que otras soluciones, y en sus últimas versiones tiene mucha optimización para alta velocidad y uso de memoria.
- Seguridad. Tiene la ventaja de trabajar sin problema con Apache web Server, el cual tienen una trayectoria probada de velocidad, confiabilidad y fuerte seguridad.
- Aplicabilidad en varias plataformas. Otras tecnologías solo son confiables al implementarlas en la misma plataforma del mismo vendedor.

5.4.4. Implementación de seguridad en el sitio

5.4.4.1. Registro de nuevo usuario

Cuando se realiza un registro y solicitud de una Cuenta del sistema de pago, éste debe ser terminado al confirmarlo por medio de una notificación que se envía al correo electrónico que se ha especificado como usuario.

De esta manera, se asegura que efectivamente la persona que realizó el registro utiliza dicha cuenta de correo.

Es esencial esta verificación, ya que el correo electrónico será en nuestro sistema de pago el identificador del cliente, y se enviarán notificaciones al mismo de toda transacción realizada.

5.4.4.2. Código de Sesión

En todos los formularios que se solicita el ingreso del correo o usuario, y la contraseña, se exige a su vez ingresar un código de sesión aleatorio que se visualiza en una imagen.

Con esto lo que se quiere evitar son los ataques simultáneos vía scritp. Así, nos aseguramos que el registro en los formularios de este tipo, los esté realizando la persona que se encuentra de frente al browser.

5.4.4.3. Creación de usuarios y contraseñas

Los usuarios o clientes son registrados en la base de datos, así como la información personal que ingresan en el registro de Cuenta.

Pero la contraseña es grabada con algoritmos de encriptación, de forma tal que nunca esa clave será desencriptada.
A su vez, en el registro de la cuenta se solicita una pregunta y una respuesta secreta, que se garantice que solo la persona que realiza el registro tiene conocimiento.

En caso de que el usuario o cliente olvide su contraseña, se solicita que responda a la pregunta secreta indicada en el registro.
Si es válida la respuesta, se solicita cambiar la contraseña.

5.4.4.4. Uso de sesiones

Cuando un usuario realiza un ingreso al sistema de pago, registra una sesión durante todo lo que realiza en el sistema.
De manera, que si el usuario quiere retornar a una página anterior sin utilizar las opciones dadas, la sesión es cancelada.

De la misma forma, al usuario siempre le solicita cerrar la sesión antes de cambiarse a otro sitio.

5.4.4.5. Controles por posibles fraudes

Cuando el usuario registra su información sensible de número de tarjeta de crédito o cuenta bancaria lo realiza una única vez.

Al registrar esta información no será visible en el navegador.

Se obligará al usuario a indicar un número de máximo de transacciones de retiro de dinero que se pueden realizar en un día, se incluye las transacciones de Retiro de Dinero, Envío de Dinero y Pagos de Productos/Servicios.

Se obligará al usuario a indicar el monto máximo permitido por transacción de retiro de dinero sea por Retiro o Envío de Dinero y un monto máximo por transacción de Pago en línea

Cuando un usuario excede el número máximo de transacciones permitidas en un día, o excede los montos máximos de acuerdo al tipo de transacción, indicados en el registro de cuenta, se realizarán las siguientes acciones:

- La primera vez, se cancelará la transacción que se pretende realizar, se notifica la falta la realizada y se envía un correo de notificación al usuario informando lo sucedido.
- La segunda vez, se cancelará la transacción que se pretende realizar, se notifica la falta realizada, se desactiva la cuenta y/o usuario y se envía un correo de notificación al usuario informando lo sucedido, con un link para la respectiva activación de la cuenta.

De esta manera, podemos minimizar el impacto en un posible caso de fraude.

5.4.5. Recorrido por el Sistema de pago electrónico.

El URL del sistema de pago electrónico es www.pagoseguro.com

Ingresado en el Explorer se puede observar lo que es la página principal o Homepage:

5.4.5.1. HomePage

Figura 8 HomePage

En el Homepage se pueden apreciar cuatro secciones:

- Informativo PagoSeguro Ecommerce

  En esta sección se explica el servicio del sistema de Pago de forma informativa de los beneficios y facilidades que brinda.

- PagoSeguro Funcionalidad

En esta sección se aprecia gráficamente las dos funcionales principales que ofrece el sistema de pago: Enviar y Recibir dinero por medio del correo

electrónico y Compra de Servicios en sitios de comercio electrónico, asi como sus actores.

Además, brinda un enlace para abrir una Cuenta Gratis, y comenzar a gozar de los beneficios del sistema.

- PagoSeguro Entidades

En esta sección se quiere incluir publicidad de las Alianzas Estratégicas que se realicen los entidades financieras para el uso de sus servicios en el sistema de pago.

- Acceso a su Cuenta

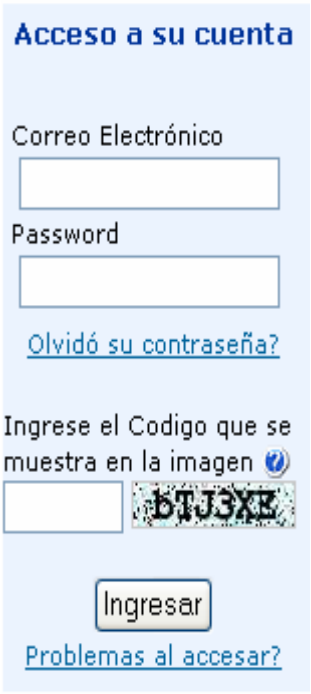
En esta sección se puede ingresar al sistema de pago, especificando el usuario y la contraseña.

Figura 9 Acceso a la cuenta

Desde el Homepage, se puede acceder a dos opciones para ingresar a PagoSeguro:

- Acceso a su Cuenta
- Abre tu cuenta Gratis
- Olvidó su contraseña

5.4.5.2. Acceso a su Cuenta



Por medio de esta opción los usuarios que tienen Cuenta de PagoSeguro realizan un login para ingresar a su Cuenta personal.

Deben especificar el correo electrónico que definieron para su Cuenta, la contraseña, y deben ingresar el Código de Seguridad que se muestra en la imagen.

Este Código permite autenticar que el usuario realmente está llenando el formulario frente al monitor, y no que está tratando de atacar el sitio con múltiples login.

Figura 10 Ingreso de user y password

Luego se presiona Ingresar. El sistema realiza las validaciones respectivas para poder permitir el acceso o denegarlo.

Figura 11 Acceso a cuenta gratis

5.4.5.3. Abrir una Cuenta

Si no eres Usuario de PagoSeguro, puedes abrir tu cuenta totalmente Gratis.

Figura 12 Tipo de cuenta

En esta pantalla se debe escoger que tipo de cuenta va a abrir:

- Cuenta Personal

Servicios: Envíos y recepción de dinero y pagos en negocios online

- Cuenta Empresarial

Servicios: Envíos y recepción de dinero y recibe pagos en línea de sus negocios en Internet.

Figura 13 Registro de cuenta personal

5.4.5.3.1. Registro de Cuenta Personal

Si se escogió la opción de Cuenta Personal, debe registrar los siguientes datos en esta pantalla:

- Nombre

- Apellidos
- Dirección
- Ciudad
- Provincia
- Código Postal
- País
- Número de Teléfono
- Correo Electrónico
- Contraseña
- Pregunta Secreta
- Respuesta Secreta
- Código de Sesión
- Aceptar Políticas de Privacidad

Figura 14 Registro de cuenta empresarial

5.4.5.3.2. Registro de Cuenta Empresarial

Si se escogió la opción de Cuenta Empresarial, debe registrar los siguientes datos en la pantalla de registro.

- Razón Social
- Dirección
- Ciudad
- Provincia

- Código Postal
- País
- Página Web
- Representante Legal
- Contacto
- Teléfono
- Correo Electrónico
- Contraseña
- Pregunta Secreta
- Respuesta Secreta
- Aceptación a las Políticas de Privacidad

Si todos los datos ingresados se validan correctamente se mostrará un mensaje de Registro Exitoso e indicando que para acceder a la cuenta debe verificar una notificación del Registro a su correo electrónico.

5.4.5.3.3. Confirmación del Registro

El usuario que se ha registrado para tener una Cuenta, si al final el registro es exitoso, recibirá una notificación a su correo electrónico en el que irá link

que estará direccionado al sitio de PagoSeguro para verificar su contraseña y acceso autorizado.

En este link, aparecerá un formulario de Confirmación de Registro en la que debe ingresar:

- contraseña válida
- código de sesión de seguridad.

Si la validación es exitosa, se permite el ingreso al sistema de pago con el usuario y contraseña indicados.

5.4.5.4. Olvidó su contraseña

Si el usuario olvidó su contraseña, por medio de esta opción puede autenticarse que efectivamente registra una cuenta en el sistema de pago y se le solicita un cambio de contraseña.

El sistema de pago no envía contraseñas por correo electrónico ni las presenta en pantalla.

Previamente el cliente debe validar su correo electrónico, la respuesta a la pregunta secreta y el código de sesión de seguridad.

5.4.6. Opciones del Sistema de Pago

Siempre que un cliente ingresa al sistema de pago, luego de la autenticación de usuario y contraseña, se presenta un home para el cliente en el que se tiene opción a una barra de opciones en la parte superior:

Figura 15 Opciones del perfil de cuenta

Las opciones disponibles son:

Mi Cuenta

Ingresar Saldo

Enviar Dinero

Retirar Dinero

Historial

Actualizar Datos

Cerrar Sesión

Figura 16 Mi perfil de cuenta

5.4.6.1. Perfil de Cuenta/Mi Cuenta

Cuando se ingresa por medio de login del HomePage, o cuando por primera vez se accede al sitio, se muestra el Perfil de la cuenta con la que se está ingresando y las opciones a las cuales puede acceder.

Se muestran dos secciones:

- **Mi Cuenta**. Aquí se presenta el Nombre, Correo Electrónico, Saldo en Cuenta, y Fecha de Ingreso.
- **5 Últimos Movimientos**. Se presentan los 5 últimos movimientos que se realizaron con la cuenta virtual. Se muestra la siguiente información por cada movimiento: Fecha, Tipo de Movimiento (Pago, Depósito, Retiro, Envío, Recepción), Remitente o Beneficiario del movimiento o transacción, Valor de la transacción, Comisión que recibe el sistema de Pago y Valor Neto de la transacción que se refleja en la cuenta bancaria o tarjeta de crédito.

Figura 17 Agregar fondos

5.4.6.2. Agregar Fondos

Esta opción permite agregar o depositar dinero en la cuenta PagoSeguro.
Se debe especificar el Monto a Depositar en dólares americanos.

Si el Usuario ingresa por primera vez a su Cuenta, debe primero ingresar la información de crédito relacionada a su cuenta PagoSeguro: Tarjeta de crédito o Cuenta Bancaria.

Puede escoger entre dos opciones de forma de pago:

- Tarjeta de Crédito
- Cuenta Bancaria

5.4.6.2.1. Registro Tarjeta de Crédito

Si es Tarjeta de Crédito debe especificar la siguiente información:

- Tarjeta de Crédito, la entidad emisora.
- Nombre del Titular
- Número de Tarjeta (mostrada en asteriscos)
- Dirección de factura
- Fecha de expiración

- Monto máximo en Retiros
- Monto máximo en Pagos
- Número máximo de retiros por día

Si la información ingresada se verifica positivamente contra los servidores de las entidades emisoras de tarjetas de crédito correspondiente, esta información queda relacionada con la cuenta PagoSeguro en adelante.

De existir cualquier validación negativa, no se podrá continuar con la transacción.

5.4.6.2.2. Registro de Cuenta Bancaria

Para el registro de Cuenta Bancaria se debe especificar la siguiente información:

- Entidad Financiera
- Tipo de Cuenta: Ahorros o Corriente
- Nombre del Titular
- Dirección de Factura
- Monto máximo en Retiros
- Monto máximo en Pagos

- Número máximo de retiros por día

Si la información ingresada se verifica positivamente contra los servidores de las entidades financieras correspondientes, esta información queda relacionada con la cuenta PagoSeguro en adelante.

De existir cualquier validación negativa, no se podrá continuar con la transacción.

Si el registro de la Cuenta Crediticia es correcto, se procede a especificar el Monto en Dólares Americanos, que se desea depositar en la cuenta PagoSeguro.

Figura 18 Retirar fondos

5.4.6.3. Retirar Dinero

Esta opción permite retirar dinero de la cuenta PagoSeguro y acreditado a la cuenta bancaria o tarjeta de crédito relacionada.

Se debe especificar el Monto a Retirar en dólares americanos.

El sistema validará que exista Saldo Suficiente para realizar la transacción.

Figura 19 Envío de dinero

5.4.6.4. Enviar Dinero

Esta opción permite Enviar Dinero a una persona, indicando su correo electrónico.

El Destinatario no necesariamente debe tener cuenta en PagoSeguro.

La información que se debe especificar en este formulario es:

- Correo electrónico del Beneficiario o quien recibe el dinero.
- Nombre del Beneficiario
- Valor o Monto a enviar (en dólares americanos).

El sistema de pago verificará que la cuenta virtual tenga saldo suficiente para realizar la transacción y enviará notificaciones tanto al cliente como al correo electrónico del beneficiario para que proceda a recibir el dinero.

El beneficiario puede o ser cliente de PagoSeguro, pero para poder recibir el dinero debe registrarse como cliente del sistema.

Figura 20 Consulta de movimientos

5.4.6.5. Historial

Esta opción permite consultar los movimientos de la cuenta PagoSeguro, por fechas y por tipo de movimiento.

5.4.6.6. Actualizar Datos

Esta opción permite realizar actualización de datos:

- Actualización de Dirección / Teléfono
- Actualización de Correo Electrónico
- Cambio de Contraseña
- Actualización de Datos Crédito (Cuenta Real)

5.4.6.6.1. Actualización de Dirección y/o Teléfono

Por medio de esta opción, el cliente puede realizar cambios de dirección y/o teléfono.

El sistema de pago validará que la dirección actualizada corresponda a la que el cliente tiene registrada en su tarjeta de crédito o en su cuenta bancaria en la institución financiera que corresponda.

5.4.6.6.2. Actualización de Correo Electrónico

Por medio de esta opción, el cliente puede realizar un cambio del Correo Electrónico de su cuenta. Si se valida el cambio de forma exitosa, todos los movimientos de la cuenta virtual quedarán relacionados a la nueva cuenta de correo.

5.4.6.6.3. Cambio de Contraseña

El cliente puede realizar un cambio de contraseña de su cuenta por medio de esta opción.

Para que el cambio se exitoso, deberá validar la contraseña actual, responder a la pregunta secreta correctamente e ingresar el código de sesión válido.

5.4.6.6.4. Actualización de Datos Crédito

El cliente puede realizar un cambio de tarjeta de crédito o de cuenta bancaria por medio de esta opción.

El sistema de pago realizará las mismas validaciones que se hacen en el registro, pero con la nueva información.

Si es correcta, se realizará una notificación del cambio, y cualquier nuevo movimiento será registrado a la nueva información.

5.4.6.6.5. Cerrar Sesión

Si el cliente desea salir del sistema de pago, debe utilizar esta opción.
Por medio de ella, el cliente regresará al homepage del sistema de pago, y se cancelará la sesión abierta.

5.4.6.7. Pago en línea

Cuando un sitio de comercio electrónico es afiliado al sistema de PagoSeguro, éste entre las opciones de forma de pago de cualquier compra o transacción debe presentar un botón que identifica que el cliente puede pagar a través del sistema PagoSeguro.

Una vez que el cliente escoge esta forma de pago, se activa una sesión con el sistema de PagoSeguro, en la que se muestra: Nombre del establecimiento, correo electrónico del establecimiento registrado en el sistema de pago, número de orden de compra o factura, descripción del bien o servicio y monto de la transacción.

El cliente debe ingresar su información de la cuenta: correo electrónico y contraseña.

Si la autenticación es exitosa, el sistema de PagoSeguro verificará si el cliente tiene saldo suficiente en su cuenta virtual para cancelar la compra.

Si es así, se realizan las transacciones de débito y crédito tanto para el comprador como el establecimiento respectivamente a sus cuentas virtuales en el sistema de pago y se notificará vía correo electrónico lo realizado.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El sistema de pagos electrónicos en línea, hoy en día es una gran solución informática que existe al alcance de todos los usuarios con acceso a Internet, brindando una gran facilidad, rapidez y actualización de sus transacciones en tiempo real de las compras y ventas en Internet, estableciendo una relación cliente y empresa muy satisfactoria y sin necesidad de ir a un local o centro comercial donde adquirir el producto.

Con este sistema se brinda al usuario la oportunidad de tener confianza para realizar sus compras en la Internet de manera segura, ya que tanto los clientes web, es decir los usuarios, transmiten su información de manera segura, y las transacciones que se realizan entre nuestro sistema y las entidades financieras también son comunicaciones seguras.

La utilización de software de código abierto durante la implementación de este sitio no contrae mayores costos de inversión, es decir casi nulo, pero en cambio sí se necesita de cierto grado de conocimiento, un tanto avanzado, como para quienes desarrollan la aplicación como también para los que diseñan e implementan la infraestructura de la red.

Las herramientas que nos permiten realizar análisis de seguridades, así como también aquellas que nos permiten implantar seguridades son necesarias para complementar la seguridad en la infraestructura de la red y durante el funcionamiento del sitio del sistema de pagos electrónicos. Es decir el constante monitoreo evita o minimiza los riesgos de infiltración, y por tanto disminuye el riesgo de pérdida para el negocio.

Recomendaciones

Partamos del hecho que las amenazas en el mundo de la informática son cada vez más frecuentes y complejas, y una violación a la seguridad podría ser devastadora para una empresa al afectar sus operaciones, la reputación corporativa y la confianza de los clientes y accionistas. Por eso es importante que las empresas implementen suficientes controles de seguridad y que tomen conciencia de su responsabilidad al administrar los datos e información tanto de la compañía como la de sus clientes.

Implementar estrictas medidas de seguridad en cada uno de los equipos y personas involucradas desde el inicio hasta el final de la puesta en línea de este sistema de pagos electrónicos.

Para la configuración de cada uno de los equipos y servidores, se deben realizar comunicaciones seguras, es decir, mantener encriptado el canal por el medio que se transmite toda clase de información del usuario y contraseña de acceso a cada uno de los equipos en la infraestructura de red, de ser posible.

Mantener un constante monitoreo y mantenimiento de la usabilidad del sistema de pagos electrónicos, de tal manera que siempre sea agradable al usuario y de esta manera atraer cada vez más usuarios nuevos y mantener los exisitentes.

Establecer políticas de marketing para los usuarios usando las mismas tecnologías de información, mediante correos electrónicos personalizados. Recopilar la información de las preferencias del usuario de tal manera que se le pueda sugerir sitios de e-commerce nuevos al usuario cada vez que inicia la sesión en el sitio.

Para constatar el grado de protección que tiene la infraestructura de red y el sitio web, es necesario realizar pruebas exhaustivas de seguridad y mejor aún por personas ajenas al desarrollo y administración del mismo, de tal

manera que se pueda verificar las posibles vulnerabilidades que se encuentren y corregirlas a tiempo, antes de poner en línea el sistema.

APÉNDICES

PANTALLAS DE CONFIGURACIÓN DE FIREWALL SUNSCREEN

Aquí se muestran cada una de las reglas configuradas en el firewall SunScreen de Solaris, implementadas en el servidor firewall que protege la capa de contenido y la capa de aplicación y servicios web.

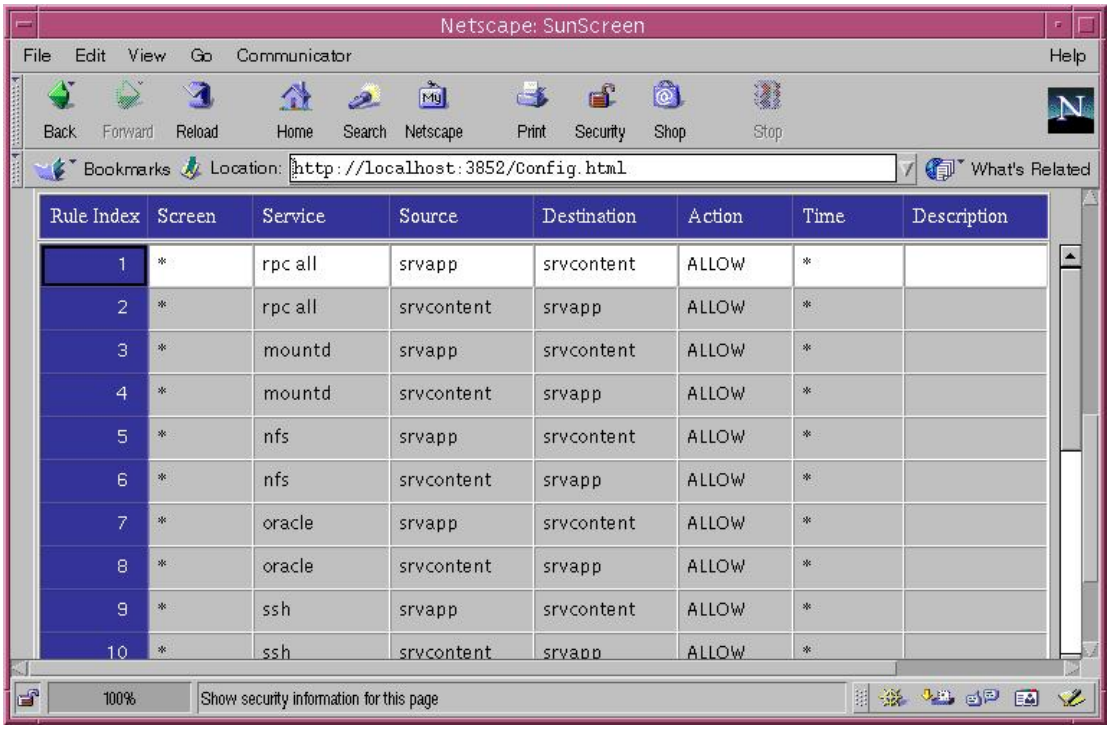


Figura 21 Primera parte de reglas del firewall

A continuación se muestra la segunda parte de la imagen captada de la reglas de configuración del firewall SunScreen.

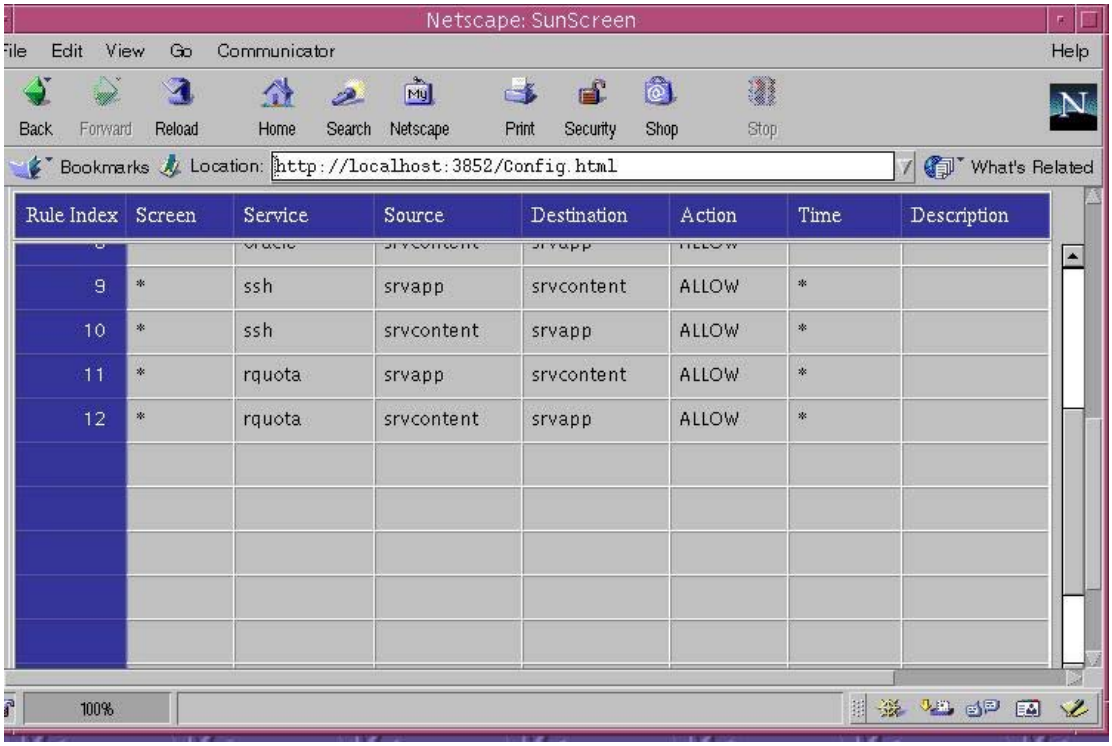


Figura 22 Segunda parte de reglas del firewall

ARCHIVO DE CONFIGURACION DEL IDS

A continuación mostramos el archivo de configuración (snort.conf) que se modificó para obtener la configuración apropiada como IDS basado en red, para detectar posibles intrusiones en la región demilitarizada de la red.

El comando que se ejecutó para tal configuración es el siguiente:
./snort –dev -c snort.conf

```
#--------------------------------------------------
#   http://www.snort.org     Snort 2.3.0 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
# $Id: snort.conf,v 1.144.2.6 2005/01/13 20:36:20 jhewlett Exp $
#
##################################################
# This file contains a sample snort configuration.
# You can take the following steps to create your own custom configuration:
#
#  1) Set the network variables for your network
#  2) Configure preprocessors
#  3) Configure output plugins
#  4) Customize your rule set
#
##################################################
# Step #1: Set the network variables:
#
# You must change the following variables to reflect your local network. The
# variable is currently setup for an RFC 1918 address space.
#
# You can specify it explicitly as:
#
# var HOME_NET 10.1.1.0/24
#
# or use global variable $<interfacename>_ADDRESS which will be always
# initialized to IP address and netmask of the network interface which you run
# snort at.  Under Windows, this must be specified as
# $(<interfacename>_ADDRESS), such as:
# $(\Device\Packet_{12345678-90AB-CDEF-1234567890AB}_ADDRESS)
#
# var HOME_NET $eth0_ADDRESS
#
# You can specify lists of IP addresses for HOME_NET
```

```
# by separating the IPs with commas like this:
#
# var HOME_NET [10.1.1.0/24,192.168.1.0/24]
#
# MAKE SURE YOU DON'T PLACE ANY SPACES IN YOUR LIST!
#
# or you can specify the variable to be any IP address
# like this:

var HOME_NET 192.168.2.0/24

# Set up the external network addresses as well.  A good start may be "any"
var EXTERNAL_NET any

# Configure your server lists.  This allows snort to only look for attacks to
# systems that have a service up.  Why look for HTTP attacks if you are not
# running a web server?  This allows quick filtering based on IP addresses
# These configurations MUST follow the same configuration scheme as defined
# above for $HOME_NET.

# List of DNS servers on your network
var DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
var SMTP_SERVERS $HOME_NET

# List of web servers on your network
#var HTTP_SERVERS $HOME_NET
var HTTP_SERVERS 192.168.2.128

# List of sql servers on your network
#var SQL_SERVERS $HOME_NET

# List of telnet servers on your network
#var TELNET_SERVERS $HOME_NET

# List of snmp servers on your network
#var SNMP_SERVERS $HOME_NET

# Configure your service ports.  This allows snort to look for attacks destined
# to a specific application only on the ports that application runs on.  For
# example, if you run a web server on port 8081, set your HTTP_PORTS variable
```

```
# like this:
#
# var HTTP_PORTS 8081
#
# Port lists must either be continuous [eg 80:8080], or a single port [eg 80].
# We will adding support for a real list of ports in the future.

# Ports you run web servers on
#
# Please note:  [80,8080] does not work.
# If you wish to define multiple HTTP ports,
#
## var HTTP_PORTS 80
## include somefile.rules
## var HTTP_PORTS 8080
## include somefile.rules
var HTTP_PORTS 80

# Ports you want to look for SHELLCODE on.
var SHELLCODE_PORTS !80

# Ports you do oracle attacks on
var ORACLE_PORTS 1521

# other variables
#
# AIM servers.  AOL has a habit of adding new AIM servers, so instead of
# modifying the signatures when they do, we add them to this list of servers.
#var                                                    AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,2
05.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/2
4,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
#var RULE_PATH ../rules
var RULE_PATH /tmp/snort-2.3.0/rules
# Configure the snort decoder
# ============================
#
# Snort's decoder will alert on lots of things such as header
# truncation or options of unusual length or infrequently used tcp options
#
```

```
#
# Stop generic decode events:
#
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
#
# config disable_tcpopt_experimental_alerts
#
# Stop Alerts on obsolete TCP options
#
# config disable_tcpopt_obsolete_alerts
#
# Stop Alerts on T/TCP alerts
#
# In snort 2.0.1 and above, this only alerts when a TCP option is detected
# that shows T/TCP being actively used on the network.  If this is normal
# behavior for your network, disable the next option.
#
# config disable_tcpopt_ttcp_alerts
#
# Stop Alerts on all other TCPOption type events:
#
# config disable_tcpopt_alerts
#
# Stop Alerts on invalid ip options
#
# config disable_ipopt_alerts

# Configure the detection engine
# ==============================
#
# Use a different pattern matcher in case you have a machine with very
limited
# resources:
#
# config detection: search-method lowmem

# Configure Inline Resets
# =======================
#
# If running an iptables firewall with snort in InlineMode() we can now
# perform resets via a physical device. We grab the indev from iptables
# and use this for the interface on which to send resets. This config
```

```
# option takes an argument for the src mac address you want to use in the
# reset packet.  This way the bridge can remain stealthy. If the src mac
# option is not set we use the mac address of the indev device. If we
# don't set this option we will default to sending resets via raw socket,
# which needs an ipaddress to be assigned to the int.
#
# config layer2resets: 00:06:76:DD:5F:E3

##################################################
# Step #2: Configure preprocessors
#
# General configuration for preprocessors is of
# the form
# preprocessor <name_of_processor>: <configuration_options>

# Configure Flow tracking module
# ------------------------------
#
# The Flow tracking module is meant to start unifying the state keeping
# mechanisms of snort into a single place. Right now, only a portscan detector
# is implemented but in the long term,  many of the stateful subsystems of
# snort will be migrated over to becoming flow plugins. This must be enabled
# for flow-portscan to work correctly.
#
# See README.flow for additional information
#
preprocessor flow: stats_interval 0 hash 2

# frag2: IP defragmentation support
# ------------------------------
# This preprocessor performs IP defragmentation.  This plugin will also detect
# people launching fragmentation attacks (usually DoS) against hosts.  No
# arguments loads the default configuration of the preprocessor, which is a 60
# second timeout and a 4MB fragment buffer.

# The following (comma delimited) options are available for frag2
#    timeout [seconds] - sets the number of [seconds] that an unfinished
#                        fragment will be kept around waiting for completion,
#                        if this time expires the fragment will be flushed
#    memcap [bytes] - limit frag2 memory usage to [number] bytes
#                     (default:  4194304)
#
#    min_ttl [number] - minimum ttl to accept
```

```
#
#    ttl_limit [number] - difference of ttl to accept without alerting
#                         will cause false positves with router flap
#
# Frag2 uses Generator ID 113 and uses the following SIDS
# for that GID:
#  SID     Event description
# -----   -------------------
#   1       Oversized fragment (reassembled frag > 64k bytes)
#   2       Teardrop-type attack

preprocessor frag2

# stream4: stateful inspection/stream reassembly for Snort
#---------------------------------------------------------------------
# Use in concert with the -z [all|est] command line switch to defeat stick/snot
# against TCP rules.  Also performs full TCP stream reassembly, stateful
# inspection of TCP streams, etc.  Can statefully detect various portscan
# types, fingerprinting, ECN, etc.

# stateful inspection directive
# no arguments loads the defaults (timeout 30, memcap 8388608)
# options (options are comma delimited):
#   detect_scans - stream4 will detect stealth portscans and generate alerts
#                  when it sees them when this option is set
#   detect_state_problems - detect TCP state problems, this tends to be very
#                           noisy because there are a lot of crappy ip stack
#                           implementations out there
#
#   disable_evasion_alerts - turn off the possibly noisy mitigation of
#                            overlapping sequences.
#
#
#   min_ttl [number]       - set a minium ttl that snort will accept to
#                            stream reassembly
#
#   ttl_limit [number]     - differential of the initial ttl on a session versus
#                            the normal that someone may be playing games.
#                            Routing flap may cause lots of false positives.
#
#   keepstats [machine|binary] - keep session statistics, add "machine" to
#                           get them in a flat format for machine reading, add
#                           "binary" to get them in a unified binary output
#                           format
```

```
#   noinspect - turn off stateful inspection only
#   timeout [number] - set the session timeout counter to [number] seconds,
#                   default is 30 seconds
#   memcap [number] - limit stream4 memory usage to [number] bytes
#   log_flushed_streams - if an event is detected on a stream this option will
#                     cause all packets that are stored in the stream4
#                     packet buffers to be flushed to disk.  This only
#                     works when logging in pcap mode!
#
# Stream4 uses Generator ID 111 and uses the following SIDS
# for that GID:
#  SID     Event description
# -----   ------------------
#   1       Stealth activity
#   2       Evasive RST packet
#   3       Evasive TCP packet retransmission
#   4       TCP Window violation
#   5       Data on SYN packet
#   6       Stealth scan: full XMAS
#   7       Stealth scan: SYN-ACK-PSH-URG
#   8       Stealth scan: FIN scan
#   9       Stealth scan: NULL scan
#   10      Stealth scan: NMAP XMAS scan
#   11      Stealth scan: Vecna scan
#   12      Stealth scan: NMAP fingerprint scan stateful detect
#   13      Stealth scan: SYN-FIN scan
#   14      TCP forward overlap

#preprocessor stream4: disable_evasion_alerts
preprocessor stream4: detect_scans

# tcp stream reassembly directive
# no arguments loads the default configuration
#   Only reassemble the client,
#   Only reassemble the default list of ports (See below),
#   Give alerts for "bad" streams
#
# Available options (comma delimited):
#   clientonly - reassemble traffic for the client side of a connection only
#   serveronly - reassemble traffic for the server side of a connection only
#   both - reassemble both sides of a session
#   noalerts - turn off alerts from the stream reassembly stage of stream4
#   ports [list] - use the space separated list of ports in [list], "all"
#                 will turn on reassembly for all ports, "default" will turn
```

```
#               on reassembly for ports 21, 23, 25, 53, 80, 143, 110, 111
#               and 513

preprocessor stream4_reassemble

# http_inspect: normalize and detect HTTP traffic and protocol anomalies
#
# lots of options available here. See doc/README.http_inspect.
# unicode.map should be wherever your snort.conf lives, or given
# a full path to where snort can find it.
preprocessor http_inspect: global \
   iis_unicode_map unicode.map 1252

preprocessor http_inspect_server: server default \
   profile apache ports { 80 } oversize_dir_length 500

#
#  Example unique server configuration
#
#preprocessor http_inspect_server: server 1.1.1.1 \
#    ports { 80 3128 8080 } \
#    flow_depth 0 \
#    ascii no \
#    double_decode yes \
#    non_rfc_char { 0x00 } \
#    chunk_length 500000 \
#    non_strict \
#    oversize_dir_length 300 \
#    no_alerts


# rpc_decode: normalize RPC traffic
# ---------------------------------
# RPC may be sent in alternate encodings besides the usual 4-byte encoding
# that is used by default. This plugin takes the port numbers that RPC
# services are running on as arguments - it is assumed that the given ports
# are actually running this type of service. If not, change the ports or turn
# it off.
# The RPC decode preprocessor uses generator ID 106
#
# arguments: space separated list
# alert_fragments - alert on any rpc fragmented TCP data
# no_alert_multiple_requests - don't alert when >1 rpc query is in a packet
# no_alert_large_fragments - don't alert when the fragmented
```

```
#                       sizes exceed the current packet size
# no_alert_incomplete - don't alert when a single segment
#                     exceeds the current packet size

preprocessor rpc_decode: 111 32771

# bo: Back Orifice detector
# ------------------------
# Detects Back Orifice traffic on the network.  Takes no arguments in 2.0.
#
# The Back Orifice detector uses Generator ID 105 and uses the
# following SIDS for that GID:
#  SID     Event description
# -----   -------------------
#   1       Back Orifice traffic detected

preprocessor bo

# telnet_decode: Telnet negotiation string normalizer
# ---------------------------------------------------
# This preprocessor "normalizes" telnet negotiation strings from telnet and ftp
# traffic.  It works in much the same way as the http_decode preprocessor,
# searching for traffic that breaks up the normal data stream of a protocol and
# replacing it with a normalized representation of that traffic so that the
# "content" pattern matching keyword can work without requiring
modifications.
# This preprocessor requires no arguments.
# Portscan uses Generator ID 109 and does not generate any SID currently.

preprocessor telnet_decode

# Flow-Portscan: detect a variety of portscans
# --------------------------------------
# Note:  The Flow preprocessor (above) must first be enabled for Flow-
Portscan to
# work.
#
# This module detects portscans based off of flow creation in the flow
# preprocessors.  The goal is to catch one->many hosts and one->many
# ports scans.
#
# Flow-Portscan has numerous options available, please read
# README.flow-portscan for help configuring this option.
```

```
# Flow-Portscan uses Generator ID 121 and uses the following SIDS for that
GID:
#  SID     Event description
# -----   ------------------
#   1       flow-portscan: Fixed Scale Scanner Limit Exceeded
#   2       flow-portscan: Sliding Scale Scanner Limit Exceeded
#   3       flow-portscan: Fixed Scale Talker Limit Exceeded
#   4        flow-portscan: Sliding Scale Talker Limit Exceeded

# preprocessor flow-portscan: \
#         talker-sliding-scale-factor 0.50 \
#         talker-fixed-threshold 30 \
#         talker-sliding-threshold 30 \
#         talker-sliding-window 20 \
#         talker-fixed-window 30 \
#         scoreboard-rows-talker 30000 \
#         server-watchnet [10.2.0.0/30] \
#         server-ignore-limit 200 \
#         server-rows 65535 \
#         server-learning-time 14400 \
#         server-scanner-limit 4 \
#         scanner-sliding-window 20 \
#         scanner-sliding-scale-factor 0.50 \
#         scanner-fixed-threshold 15 \
#         scanner-sliding-threshold 40 \
#         scanner-fixed-window 15 \
#         scoreboard-rows-scanner 30000 \
#         src-ignore-net [192.168.1.1/32,192.168.0.0/24] \
#         dst-ignore-net [10.0.0.0/30] \
#         alert-mode once \
#         output-mode msg \
#         tcp-penalties on

# sfPortscan
# ----------
# Author: Dan Roelker
# Portscan detection module.  Detects various types of portscans and
# portsweeps.  For more information on detection philosophy, alert types,
# and detailed portscan information, please refer to the README.sfportscan.
#
# -configuration options-
#     proto { tcp udp icmp ip_proto all }
#       The arguments to the proto option are the types of protocol scans that
```

```
#       the user wants to detect.  Arguments should be separated by spaces
and
#      not commas.
#     scan_type { portscan portsweep decoy_portscan distributed_portscan all
}
#      The arguments to the scan_type option are the scan types that the
#       user wants to detect.  Arguments should be separated by spaces and
not
#      commas.
#     sense_level { low|medium|high }
#      There is only one argument to this option and it is the level of
#      sensitivity in which to detect portscans.  The 'low' sensitivity
#       detects scans by the common method of looking for response errors,
such
#      as TCP RSTs or ICMP unreachables.  This level requires the least
#      tuning.  The 'medium' sensitivity level detects portscans and
#      filtered portscans (portscans that receive no response).  This
#      sensitivity level usually requires tuning out scan events from NATed
#      IPs, DNS cache servers, etc.  The 'high' sensitivity level has
#      lower thresholds for portscan detection and a longer time window than
#      the 'medium' sensitivity level.  Requires more tuning and may be noisy
#      on very active networks.  However, this sensitivity levels catches the
#      most scans.
#     memcap { positive integer }
#      The maximum number of bytes to allocate for portscan detection.  The
#      higher this number the more nodes that can be tracked.
#     logfile { filename }
#      This option specifies the file to log portscan and detailed portscan
#      values to.  If there is not a leading /, then snort logs to the
#      configured log directory.  Refer to README.sfportscan for details on
#      the logged values in the logfile.
#     watch_ip { Snort IP List }
#     ignore_scanners { Snort IP List }
#     ignore_scanned { Snort IP List }
#      These options take a snort IP list as the argument.  The 'watch_ip'
#      option specifies the IP(s) to watch for portscan.  The
#      'ignore_scanners' option specifies the IP(s) to ignore as scanners.
#      Note that these hosts are still watched as scanned hosts.  The
#      'ignore_scanners' option is used to tune alerts from very active
#      hosts such as NAT, nessus hosts, etc.  The 'ignore_scanned' option
#      specifies the IP(s) to ignore as scanned hosts.  Note that these hosts
#      are still watched as scanner hosts.  The 'ignore_scanned' option is
#      used to tune alerts from very active hosts such as syslog servers, etc.
#
```

```
preprocessor sfportscan: proto  { all } \
                    memcap { 10000000 } \
                    sense_level { low }

# arpspoof
#--------------------------------------
# Experimental ARP detection code from Jeff Nathan, detects ARP attacks,
# unicast ARP requests, and specific ARP mapping monitoring.  To make use
of
# this preprocessor you must specify the IP and hardware address of hosts
on
# the same layer 2 segment as you.  Specify one host IP MAC combo per
line.
# Also takes a "-unicast" option to turn on unicast ARP request detection.
# Arpspoof uses Generator ID 112 and uses the following SIDS for that GID:

#  SID     Event description
# -----   -------------------
#   1       Unicast ARP request
#   2       Etherframe ARP mismatch (src)
#   3       Etherframe ARP mismatch (dst)
#   4       ARP cache overwrite attack

#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00

# Performance Statistics
# ----------------------
# Documentation for this is provided in the Snort Manual.  You should read it.
# It is included in the release distribution as doc/snort_manual.pdf
#
# preprocessor perfmonitor: time 300 file /var/snort/snort.stats pktcnt 10000

##################################################################
######
# Step #3: Configure output plugins
#
# Uncomment and configure the output plugins you decide to use.  General
# configuration for output plugins is of the form:
#
# output <name_of_plugin>: <configuration_options>
#
# alert_syslog: log alerts to syslog
# ----------------------------------
```

```
# Use one or more syslog facilities as arguments.  Win32 can also optionally
# specify a particular hostname/port.  Under Win32, the default hostname is
# '127.0.0.1', and the default port is 514.
#
# [Unix flavours should use this format...]
# output alert_syslog: LOG_AUTH LOG_ALERT
#
# [Win32 can use any of these formats...]
# output alert_syslog: LOG_AUTH LOG_ALERT
# output alert_syslog: host=hostname, LOG_AUTH LOG_ALERT
# output alert_syslog: host=hostname:port, LOG_AUTH LOG_ALERT

# log_tcpdump: log packets in binary tcpdump format
# -----------------------------------------------
# The only argument is the output file name.
#
# output log_tcpdump: tcpdump.log

# database: log to a variety of databases
# ---------------------------------------
# See the README.database file for more information about configuring
# and using this plugin.
#
# output database: log, mysql, user=root password=test dbname=db
host=localhost
# output database: alert, postgresql, user=snort dbname=snort
# output database: log, odbc, user=snort dbname=snort
# output database: log, mssql, dbname=snort user=snort password=test
# output database: log, oracle, dbname=snort user=snort password=test

# unified: Snort unified binary format alerting and logging
# -------------------------------------------------------------
# The unified output plugin provides two new formats for logging and
generating
# alerts from Snort, the "unified" format.  The unified format is a straight
# binary format for logging data out of Snort that is designed to be fast and
# efficient.  Used with barnyard (the new alert/log processor), most of the
# overhead for logging and alerting to various slow storage mechanisms such
as
# databases or the network can now be avoided.
#
# Check out the spo_unified.h file for the data formats.
#
# Two arguments are supported.
```

```
#    filename - base filename to write to (current time_t is appended)
#    limit    - maximum size of spool file in MB (default: 128)
#
# output alert_unified: filename snort.alert, limit 128
# output log_unified: filename snort.log, limit 128

# You can optionally define new rule types and associate one or more output
# plugins specifically to that type.
#
# This example will create a type that will log to just tcpdump.
# ruletype suspicious
# {
#   type log
#   output log_tcpdump: suspicious.log
# }
#
# EXAMPLE RULE FOR SUSPICIOUS RULETYPE:
# suspicious tcp $HOME_NET any -> $HOME_NET 6667 (msg:"Internal IRC
Server";)
#
# This example will create a rule type that will log to syslog and a mysql
# database:
# ruletype redalert
# {
#   type alert
#   output alert_syslog: LOG_AUTH LOG_ALERT
#   output database: log, mysql, user=snort dbname=snort host=localhost
# }
#
# EXAMPLE RULE FOR REDALERT RULETYPE:
# redalert tcp $HOME_NET any -> $EXTERNAL_NET 31337 \
#   (msg:"Someone is being LEET"; flags:A+;)

#
# Include classification & priority settings
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\etc\classification.config
#

include classification.config

#
# Include reference systems
# Note for Windows users:  You are advised to make this an absolute path,
```

```
# such as:  c:\snort\etc\reference.config
#

include reference.config

##################################################################
######
# Step #4: Customize your rule set
#
# Up to date snort rules are available at http://www.snort.org
#
# The snort web site has documentation about how to write your own custom
snort
# rules.
#
# The rules included with this distribution generate alerts based on on
# suspicious activity. Depending on your network environment, your security
# policies, and what you consider to be suspicious, some of these rules may
# either generate false positives ore may be detecting activity you consider to
# be acceptable; therefore, you are encouraged to comment out rules that are
# not applicable in your environment.
#
# The following individuals contributed many of rules in this distribution.
#
# Credits:
#   Ron Gula <rgula@securitywizards.com> of Network Security Wizards
#   Max Vision <vision@whitehats.com>
#   Martin Markgraf <martin@mail.du.gtn.com>
#   Fyodor Yarochkin <fygrave@tigerteam.net>
#   Nick Rogness <nick@rapidnet.com>
#   Jim Forster <jforster@rapidnet.com>
#   Scott McIntyre <scott@whoi.edu>
#   Tom Vandepoel <Tom.Vandepoel@ubizen.com>
#   Brian Caswell <bmc@snort.org>
#   Zeno <admin@cgisecurity.com>
#   Ryan Russell <ryan@securityfocus.com>



#==================================
# Include all relevant rulesets here
#
# The following rulesets are disabled by default:
#
```

```
#   web-attacks, backdoor, shellcode, policy, porn, info, icmp-info, virus,
#   chat, multimedia, and p2p
#
# These rules are either site policy specific or require tuning in order to not
# generate false positive alerts in most enviornments.
#
# Please read the specific include file for more information and
# README.alert_order for how rule ordering affects how alerts are triggered.
#========================================

include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules

include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-php.rules

include $RULE_PATH/sql.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/oracle.rules
include $RULE_PATH/mysql.rules
include $RULE_PATH/snmp.rules

include $RULE_PATH/smtp.rules
include $RULE_PATH/imap.rules
```

```
include $RULE_PATH/pop2.rules
include $RULE_PATH/pop3.rules

include $RULE_PATH/nntp.rules
include $RULE_PATH/other-ids.rules
# include $RULE_PATH/web-attacks.rules
# include $RULE_PATH/backdoor.rules
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
# include $RULE_PATH/porn.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
 include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/p2p.rules
include $RULE_PATH/experimental.rules

# Include any thresholding or suppression commands. See threshold.conf in
the
# <snort src>/etc directory for details. Commands don't necessarily need to
be
# contained in this conf, but a separate conf makes it easier to maintain them.
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\etc\threshold.conf
# Uncomment if needed.
# include threshold.conf
```

CONFIGURACIÓN DE SEGURIDAD EN LA BASE DE DATOS

Para proteger los datos y estructura de la base de datos, se ha utilizado lo que se llama en Oracle, Privilegios de Sistema y Roles.

Privilegios de Sistema

Permite que los usuarios ejecuten operaciones particulares sobre la base de datos. Estas incluyen creación, eliminación o modificación de tablas, vistas, segmentos de rollback y procedimientos.

Roles

Los Roles son grupos de privilegios relacionados que se conceden a usuarios u otros roles.

De acuerdo a estos conceptos se realizó la siguiente estructura y definición de usuarios, roles y privilegios en la base de datos:

El usuario dueño de los objetos es: “pagoseg”.

1. Creación de usuarios funcionales.

Se creará un usuario sinónimo por cada función u opción en la aplicación.

Se creará un usuario sinónimo genérico para la navegación.

Usuario genérico (navegación por páginas informativas, registro)

CREATE genuser SYNONYM cl_usuarios for pagoseg.cl_usuarios;

CREATE genuser SYNONYM cl_clientes for pagoseg.cl_usuarios;

CREATE genuser SYNONYM cl_datos_credito for pagoseg.cl_usuarios;

CREATE genuser SYNONYM tr_movimiento_cv for pagoseg.cl_usuarios;

CREATE genuser SYNONYM tr_movimiento_cr for pagoseg.cl_usuarios;

CREATE genuser SYNONYM tr_movimiento_pendiente for pagoseg.cl_usuarios;

CREATE genuser SYNONYM tr_creditos for pagoseg.cl_usuarios;

CREATE genuser SYNONYM tr_pagos for pagoseg.cl_usuarios;

CREATE genuser SYNONYM tr_saldos_cv for pagoseg.cl_usuarios;

CREATE genuser SYNONYM si_tarjetas_credito for pagoseg.cl_usuarios;

CREATE genuser SYNONYM si_cuenta_bancaria for pagoseg.cl_usuarios;

Usuario de consulta (perfil, movimientos)

CREATE conuserSYNONYM cl_usuarios for pagoseg.cl_usuarios;

CREATE conuser SYNONYM cl_clientes for pagoseg.cl_usuarios;

CREATE conuser SYNONYM cl_datos_credito for pagoseg.cl_usuarios;

CREATE conuser SYNONYM tr_movimiento_cv for pagoseg.cl_usuarios;

CREATE conuser SYNONYM tr_movimiento_cr for pagoseg.cl_usuarios;

CREATE conuser SYNONYM tr_movimiento_pendiente for pagoseg.cl_usuarios;

CREATE conuser SYNONYM tr_creditos for pagoseg.cl_usuarios;

CREATE conuser SYNONYM tr_pagos for pagoseg.cl_usuarios;

CREATE conuser SYNONYM tr_saldos_cv for pagoseg.cl_usuarios;

CREATE conuser SYNONYM si_tarjetas_credito for pagoseg.cl_usuarios;

CREATE conuser SYNONYM si_cuenta_bancaria for pagoseg.cl_usuarios;

Usuario para agregar fondos

CREATE agruser SYNONYM cl_usuarios for pagoseg.cl_usuarios;

CREATE agruser SYNONYM cl_clientes for pagoseg.cl_usuarios;

CREATE agruser SYNONYM cl_datos_credito for pagoseg.cl_usuarios;

CREATE agruser SYNONYM tr_movimiento_cv for pagoseg.cl_usuarios;

CREATE agruser SYNONYM tr_movimiento_cr for pagoseg.cl_usuarios;

CREATE agruser SYNONYM tr_movimiento_pendiente for pagoseg.cl_usuarios;

CREATE agruser SYNONYM tr_creditos for pagoseg.cl_usuarios;

CREATE agruser SYNONYM tr_pagos for pagoseg.cl_usuarios;

CREATE agruser SYNONYM tr_saldos_cv for pagoseg.cl_usuarios;

CREATE agruser SYNONYM si_tarjetas_credito for pagoseg.cl_usuarios;

CREATE agruser SYNONYM si_cuenta_bancaria for pagoseg.cl_usuarios;

Usuario para retirar fondos

CREATE retuser SYNONYM cl_usuarios for pagoseg.cl_usuarios;

CREATE retuser SYNONYM cl_clientes for pagoseg.cl_usuarios;

CREATE retuser SYNONYM cl_datos_credito for pagoseg.cl_usuarios;

CREATE retuser SYNONYM tr_movimiento_cv for pagoseg.cl_usuarios;

CREATE retuser SYNONYM tr_movimiento_cr for pagoseg.cl_usuarios;

CREATE retuser SYNONYM tr_movimiento_pendiente for pagoseg.cl_usuarios;

CREATE retuser SYNONYM tr_creditos for pagoseg.cl_usuarios;

CREATE retuser SYNONYM tr_pagos for pagoseg.cl_usuarios;

CREATE retuser SYNONYM tr_saldos_cv for pagoseg.cl_usuarios;

CREATE retuser SYNONYM si_tarjetas_credito for pagoseg.cl_usuarios;

CREATE retuser SYNONYM si_cuenta_bancaria for pagoseg.cl_usuarios;

Usuario para enviar dinero

CREATE envuser SYNONYM cl_usuarios for pagoseg.cl_usuarios;

CREATE envuser SYNONYM cl_clientes for pagoseg.cl_usuarios;

CREATE envuser SYNONYM cl_datos_credito for pagoseg.cl_usuarios;

CREATE envuser SYNONYM tr_movimiento_cv for pagoseg.cl_usuarios;

CREATE envuser SYNONYM tr_movimiento_cr for pagoseg.cl_usuarios;

CREATE envuser SYNONYM tr_movimiento_pendiente for pagoseg.cl_usuarios;

CREATE envuser SYNONYM tr_creditos for pagoseg.cl_usuarios;

CREATE envuser SYNONYM tr_pagos for pagoseg.cl_usuarios;

CREATE envuser SYNONYM tr_saldos_cv for pagoseg.cl_usuarios;

CREATE envuser SYNONYM si_tarjetas_credito for pagoseg.cl_usuarios;

CREATE envuser SYNONYM si_cuenta_bancaria for pagoseg.cl_usuarios;

Usuario para realizar pagos

CREATE paguser SYNONYM cl_usuarios for pagoseg.cl_usuarios;

CREATE paguser SYNONYM cl_clientes for pagoseg.cl_usuarios;

CREATE paguser SYNONYM cl_datos_credito for pagoseg.cl_usuarios;

CREATE paguser SYNONYM tr_movimiento_cv for pagoseg.cl_usuarios;

CREATE paguser SYNONYM tr_movimiento_cr for pagoseg.cl_usuarios;

CREATE paguser SYNONYM tr_movimiento_pendiente for pagoseg.cl_usuarios;

CREATE paguser SYNONYM tr_creditos for pagoseg.cl_usuarios;

CREATE paguser SYNONYM tr_pagos for pagoseg.cl_usuarios;

CREATE paguser SYNONYM tr_saldos_cv for pagoseg.cl_usuarios;

CREATE paguser SYNONYM si_tarjetas_credito for pagoseg.cl_usuarios;

CREATE paguser SYNONYM si_cuenta_bancaria for pagoseg.cl_usuarios;

2. Creación de Roles

Se crean los Roles conectado con el usuario SYSTEM.

```
CREATE ROLE navegador;

CREATE ROLE cliente;
```

3. Asignación de Privilegios

Se asignan los Privilegios de los objetos a los roles conectado con usuario PAGOSEG.

Rol Navegador

```
GRANT select ON cl_usuarios to navegador;

GRANT insert ON  cl_usuarios to navegador;

GRANT update ON  cl_usuarios to navegador;

GRANT select ON cl_clientes to navegador;

GRANT insert ON  cl_clientes to navegador;

GRANT update ON  cl_clientes to navegador;

GRANT execute ON  cl_crear_cliente to navegador;

GRANT execute ON  cl_crear_cuenta to navegador;

GRANT execute ON  cl_existe_cuenta to navegador;
```

Rol Cliente

```
GRANT select ON cl_usuarios to cliente;

GRANT update ON  cl_usuarios to cliente;
```

```
GRANT select ON cl_clientes to cliente;

GRANT update ON  cl_clientes to cliente;

GRANT select ON cl_datos_credito to cliente;

GRANT update ON  cl_datos_credito to cliente;

GRANT insert ON  cl_datos_credito to cliente;

GRANT select ON cl_datos_credito to cliente;

GRANT update ON  cl_datos_credito to cliente;

GRANT insert ON  cl_datos_credito to cliente;

GRANT select ON tr_movimiento_cv to cliente;

GRANT update ON  tr_movimiento_cv to cliente;

GRANT insert ON  tr_movimiento_cv to cliente;

GRANT select ON tr_movimiento_cr to cliente;

GRANT update ON  tr_movimiento_cr to cliente;

GRANT insert ON  tr_movimiento_cr to cliente;

GRANT select ON tr_movimiento_pendiente to cliente;

GRANT update ON  tr_movimiento_pendiente to cliente;

GRANT insert ON  tr_movimiento_pendiente to cliente;

GRANT select ON tr_creditos to cliente;

GRANT update ON  tr_creditos to cliente;

GRANT insert ON  tr_creditos to cliente;

GRANT select ON tr_pagos to cliente;

GRANT update ON  tr_pagos to cliente;
```

```
GRANT insert ON  tr_pagos to cliente;

GRANT select ON tr_saldos_cv to cliente;

GRANT update ON  tr_saldos_cv to cliente;

GRANT insert ON  tr_saldos_cv to cliente;

GRANT select ON si_tarjetas_credito to cliente;

GRANT update ON  si_tarjetas_credito to cliente;

GRANT insert ON  si_tarjetas_credito to cliente;

GRANT select ON si_cuenta_bancaria to cliente;

GRANT update ON  si_cuenta_bancaria to cliente;

GRANT insert ON  si_cuenta_bancaria to cliente;

GRANT execute ON  cl_verifica_credito to cliente;

GRANT execute ON  tr_agregar_fondos to cliente;

GRANT execute ON  tr_enviar_dinero to cliente;

GRANT execute ON  tr_pagar_compra to cliente;

GRANT execute ON  tr_retirar_fondos to cliente;

GRANT execute ON  tr_saldo_actual to cliente;

GRANT execute ON  cl_verificar_pendiente to cliente;

GRANT execute ON  cl_verifica_credito to cliente;
```

4. Asignación de Roles a Usuarios

```
GRANT navegador to genuser ;
```

GRANT cliente to conuser ;

GRANT cliente to paguser ;

GRANT cliente to envuser ;

GRANT cliente to retuser ;

GRANT cliente to agruser ;

CONFIGURACION DEL ROUTER CISCO 1700 DE ACCESO A INTERNET

! Last configuration change at 15:57:15 EST Tue Jan 5 2005 by admin

! NVRAM config last updated at 15:57:31 EST Tue Jan 5 2005 by admin

!

version 12.3

no service pad

service tcp-keepalives-in

service tcp-keepalives-out

service timestamps debug datetime localtime

service timestamps log datetime localtime

service password-encryption

!

hostname router srvfw02

!

```
logging buffered 51200 warnings
enable secret 5 $1$dYau$njFyCp1b1qSBlMCw3AWM2/
!
username Admin privilege 13 password 7 0518091A711D1E3F1C0B23
clock timezone EST -5
no aaa new-model
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 4000
!
!
ip flow-cache timeout active 1
no ip bootp server
ip domain name pagoseguro.com
no ftp-server write-enable
!
!
interface Null0
 no ip unreachables
!
interface Ethernet0/0
 description Interface conectada al DMZ
```

```
 ip address 192.168.2.128  255.255.255.0
 ip access-group Interface-local in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip nat inside
 ip route-cache flow
 no ip mroute-cache
 duplex full
 speed 100
 no mop enabled
!
interface Ethernet0/1
 description Interface conectada al ISP
 ip address 200.10.168.25 255.255.255.0
 ip access-group Interface-Internet in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip wccp web-cache redirect out
 ip nat outside
 ip route-cache flow
```

```
 no ip mroute-cache
 duplex full
 speed 100
 no cdp enable
 no mop enabled
!
interface Serial0/0/0
 no ip address
 no ip unreachables
 no ip proxy-arp
 no ip mroute-cache
 shutdown
 clockrate 2000000
 no cdp enable
!
router eigrp 1
 redistribute static
 passive-interface Ethernet0/1
 network 192.168.2.0 0.0.0.255
 no default-information out
 auto-summary
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 200.10.168.28

no ip http server
ip nat translation tcp-timeout 300
ip nat translation max-entries 50
no ip nat service sip tcp port 5060
no ip nat service sip udp port 5060
!
ip access-list extended Interface-Internet
 remark Restricciones segun sitio web de Cisco
 deny   icmp any any redirect
 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip 224.0.0.0 31.255.255.255 any
deny   ip host 0.0.0.0 any
 deny   udp any any eq tftp
deny   udp any any eq 135
 deny   tcp any any eq 135
 deny   udp any any eq snmp
 deny   udp any any eq snmptrap
 deny   udp any any eq netbios-ns
 deny   tcp any any eq 137
```

deny udp any any eq netbios-dgm

deny tcp any any eq 139

deny tcp any any eq 389

deny tcp any any eq 411

deny tcp any any eq 412

deny udp any any eq 445

deny tcp any any eq 445

deny tcp any any eq 1434

deny udp any any eq 1434

deny tcp any any eq 4181

deny tcp any any eq 4662

deny udp any any eq 4662

deny tcp any any eq 4672

deny udp any any eq 4672

deny tcp any any eq 6346

deny udp any any eq 6346

deny tcp any 192.168.2.0 0.0.0.255 eq telnet

deny tcp any 192.168.2.0 0.0.0.255 eq 1080

deny tcp any 192.168.2.0 0.0.0.255 eq 5900

deny tcp any 192.168.2.0 0.0.0.255 eq 8080

remark Para el acceso al Servidor Web Pago Seguro

```
 permit tcp any host 192.168.2.155 eq 22
 permit tcp any host 192.168.2.155 eq smtp
 permit tcp any host 192.168.2.155 eq www
 permit tcp any host 192.168.2.155 eq 443
remark Puertos negados de clientes Windows
 deny   udp any any eq 135
 deny   tcp any any eq 135
 deny   udp any any eq netbios-ns
 deny   tcp any any eq 137
 deny   udp any any eq netbios-dgm
 deny   tcp any any eq 139
 deny   tcp any any eq 411
 deny   tcp any any eq 412
 deny   udp any any eq 445
 deny   tcp any any eq 445

access-list 10 remark Lista de Acceso para la consola
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny   any log
!
line con 0
login local
```

ESQUEMA DE COMUNICACION Y OPERACIÓN ENTRE PAGOSEGURO Y LAS OPERADORAS

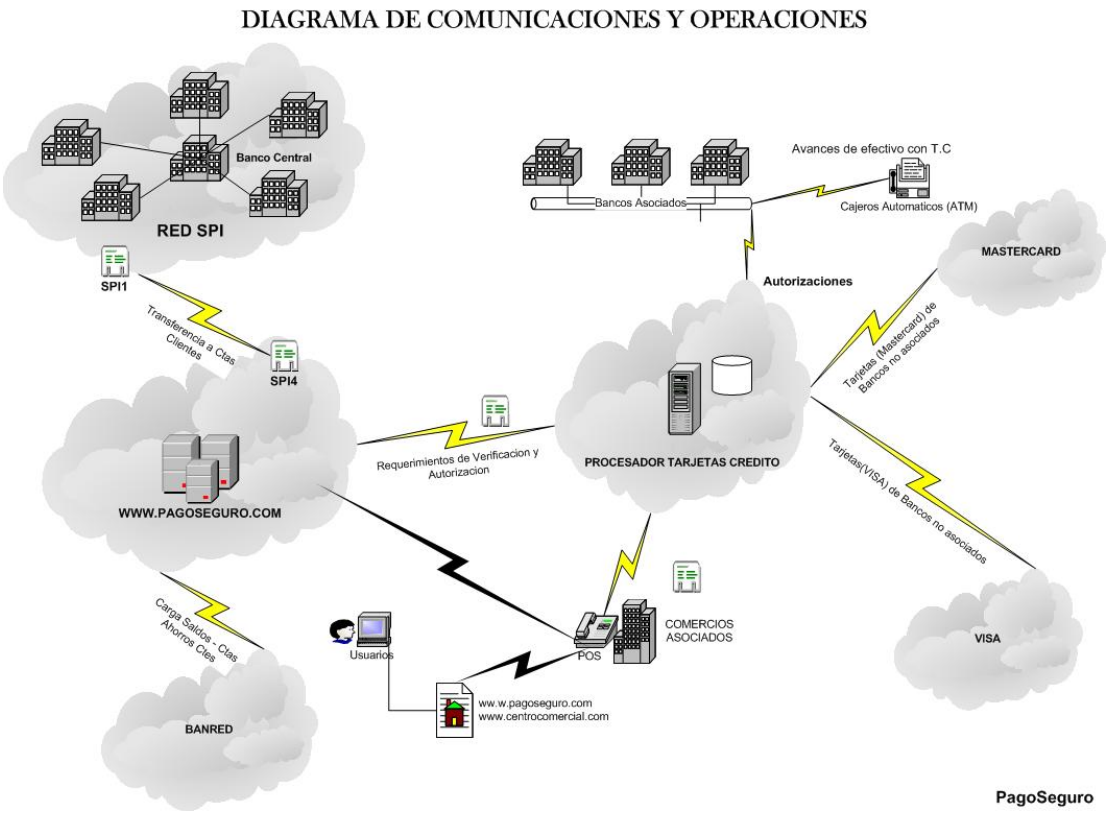


Figura 23 Diagrama de Comunicaciones y operadoras

BIBLIOGRAFIA

1 STALLINGS W., Cryptography and Network Security: Principles and practice, Prentice Hall, USA, Second Edition, 1999

2 ANONYMOUS, Maximum Security, SAMS, USA, Fourt Edition, Diciembre 2002

3 http://www.php.net

4 http://www.apache.org

5 http://www.openssl.org

6 http://www.redhat.com

7 http://docs.sun.com