DESARROLLO DE UN SITIO SEGURO DE E-COMMERCE DEDICADO A LA VENTA DE ARREGLOS FLORALES Y REGALOS ESPECIALES PARA CUALQUIER OCASION

Julio Pintag Sanga[1], Walter Ramirez Bocca[2], Steve Aguirre Wong[3], Karina Astudillo Barahona[4],

[1]Ingeniero en Computación 2005
[2]Ingeniero en Computación 2005
[3]Ingeniero en Computación 2005
[4]Directora de Tópico. Ingeniera en Computación, Escuela Superior Politécnica del Litoral. Profesora de la ESPOL desde 2002.

RESUMEN

En el presente artículo se describe la implementación y configuración de herramientas de seguridad y esquemas seguros de redes que se ha desarrollado para proteger un sitio web de e-commerce denominado “Contodomiamor.com” que ofrece el servicio de venta de arreglos florales y obsequios complementarios. En este sitio web los clientes mediante su tarjeta de crédito podrán realizar compras, procesando la transacción de manera confiable y segura.

Para la construcción del sitio seguro se han tomado en consideración los principios elementales de seguridad de información que son: la autenticación de clientes, la integridad, confidencialidad de datos y la disponibilidad de servicios en la web las 24 horas del día.

The present article describes the configuration and implementation of information technology security tools and protected network schemas developed in order to protect a web sited called “Contodomiamor.com” which deals with flowers and complimentary gifts sales. On the website the customers can make purchases through credit card, processing the transactions in a reliable and secure way.

In the design of the web site had taken in account elementary information security principles such as: customer authentication, data integrity and confidentiality and services availability 24 hours a day.

INTRODUCCIÓN

El sistema de e-commerce implementado está orientado a la venta de arreglos florales, en combinación con obsequios complementarios como: bombones, peluches, adornos, bebidas, libros, entre otros; categorizados para diferentes eventos y ocasiones.

En el diseño de la página se consideraron características como: facilidad de uso para usuarios expertos y novatos, interface agradable y desventajas de la transaccionalidad propuesta por sitios web existentes en el mercado (competencia).

El esquema de pagos implementado está basado en transacciones con tarjetas de crédito sobre un enlace de transmisión protegido; es decir, mediante un protocolo de encriptación de datos se protege la información confidencial de los clientes como: datos generales, pin de la tarjeta, contraseña, fechas de expiración y cvv2[1].

Este sistema está basado en un esquema de red seguro, minimizando el riesgo de intrusiones tanto de usuarios internos como externos, usando para aquello herramientas y estrategias de seguridad disponibles en el mercado.

1. Análisis

1.1 Análisis de Mercado

Debido a que en el Ecuador actualmente no está totalmente adoptado el esquema de compras y pagos electrónicos, se realizó una investigación de mercado para conocer las oportunidades de ingresar al mercado local existente.

El cuestionario de investigación de mercado desarrollado considera los siguientes aspectos:

- Sexo y edad.
- Costumbre de obsequiar flores.
- Los tipos de obsequios adicionales que se suelen regalar.
- Eventos en los que se obsequian flores.
- Formas de pago utilizadas.
- Costumbre de realizar compras por Internet.
- Disposición del encuestado para adquirir los productos ofrecidos por Internet.

[1] Código autorizado para transacciones cuya información no está disponible en la banda magnética de la tarjeta.

Finalmente se realizó el análisis de competidores, para saber las fortalezas y debilidades que presentan, a continuación se muestra el detalle de este estudio

Sitio Web	Fortalezas	Debilidades
www.braganca.com	➢ Interface agradable ➢ Dos esquemas de Pagos con tarjeta , en línea y vía confirmación telefónica ➢ Presenta guía para realizar los pagos. ➢ Buen posicionamiento en el mercado actual	➢ Sólo tiene cobertura en Guayaquil y Quito ➢ Precios elevados ➢ Poca variedad de productos ➢ No ofrece promociones complementarias
www.florerialamarcelle.com	➢ Presencia en el mercado no electrónico ➢ Goza de prestigio en el comercio tradicional	➢ Diseño web muy informal ➢ No brinda facilidades de observar un preliminar del arreglo floral seleccionado ➢ Sitio no amigable para clientes potenciales ➢ No ofrece pago electrónico ➢ Promociones desactualizadas
www.daflores.com	➢ Presencia en países americanos ➢ Buena interface de usuario	➢ Precios elevados ➢ Solo existen 4 opciones de arreglos ➢ Instrucciones de pagos no son claras
www.delejos.com	➢ Ofrece alternativa de pago con tarjeta de crédito ➢ Amplia cobertura en principales ciudades del Ecuador	➢ Pocas opciones de arreglos ➢ No ofrece alternativa de búsquedas en base a criterios ➢ Precios elevados ➢ Sitio web poco creativo

Tabla 1 Análisis de fortalezas y debilidades de competidores

1.2 Análisis de Requerimientos

A continuación se presentan los requerimientos o especificaciones funcionales del sitio web a implementar:

- Diseñar un sitio web orientado a la venta de arreglos florales y obsequios complementarios.
- Permitir ver todos los arreglos disponibles en el sitio organizados por tipo de obsequios y por ocasión.
- Presentar opciones de búsqueda en base a tres parámetros: destinatario, ocasión y precio.
- Permitir la creación y mantenimiento de usuarios del sitio web.
- Permitir la compra de artículos y su edición en base al esquema de carrito de compras.
- Permitir la consulta del histórico de compras realizadas.
- Permitir ingresar los datos del destinatario en la compra y personalizar el mensaje adjunto.
- Emitir el detalle de la factura.
- Permitir el pago electrónico a través de tarjetas de crédito.
- Permitir navegación informativa del sitio.

A continuación se detallan los requerimientos no funcionales o también llamadas especificaciones técnicas:

- Implementar el sitio web bajo un esquema de transmisión segura.
- Implementar un esquema de red confiable ante ataques externos maliciosos.
- Autenticar el pago mediante tarjeta de crédito de los clientes.
- Autenticación del sitio en funciones de ingreso de palabras secretas o "touring number"2
- Requerimientos de hardware/software que permitan una navegación rápida y confiable en el sitio.

Estos requerimientos no funcionales fueron definidos considerando el tipo de negocio que se va a implantar vía el esquema de comercio electrónico, considerando proteger la información ingresada por los clientes.

2. Diseño

2.1 Diseño de Red

Para el diseño se realizó dos esquemas, el primero al cual se llamará Diseño de Esquema Ideal se ha realizado pensando en maximizar la seguridad de la red sin escatimar en gastos; el segundo al cual se llamará esquema de laboratorio; es el que se ha desarrollado pensando en reducir costos de implementación, sin dejar a un lado la seguridad y de alguna manera demostrar la eficiencia de las herramientas que en el proyecto se mencionan. Cabe recalcar que ambos esquemas siguen la misma idea; la diferencia está en que el esquema de laboratorio ha sido implementado ajustándose al reducido presupuesto que se tiene para el proyecto.

2.1.1 Diseño de Esquema Ideal

En el esquema se contempla tres niveles de seguridad. La primera barrera de protección ante usuarios externos es provista por el ruteador "packet filtering"[3], a continuación del esquema se considera el firewall principal que implementa "Stateful Inspection", tecnología que revisa enteramente los paquetes descartando aquellos que presente anormalidades. Finalmente para la protección contra usuarios internos se dispone de un firewall interno. En el esquema también se implementa un Detector de intrusos, el mismo que revisa los paquetes que circulan desde y hacia Internet, revisando anormalidades, basados en patrones de ataques que se actualiza continuamente de Internet. El esquema también considera contingencia tanto de datos como de enlaces, implementando tecnologías tales como apilamiento a nivel switching[4], redundancia de enlaces y RAID a nivel de datos.

---

[2] Número generado en la página que debe ser digitado por el usuario para garantizar que el sitio es genuino y no una falsificación.

[3] Filtrador de paquetes basada en lista en accesos

[4] Conmutación de datos a nivel LAN. Terminado usado para referirse a equipos LAN denominados switch.

2.1.2 Diseño de Esquema Laboratorio

Debido a las limitaciones en cuanto a la disponibilidad de equipos y presupuesto; se diseñó una red de laboratorio, en la cual se omitió varios servidores y en otros casos se instalaron en un solo servidor varios servicios; a pesar de eso la red implementada ofrece los suficientes niveles de seguridad para poder demostrar la eficiencia de las tecnologías utilizadas.

A continuación se muestra un diagrama con los elementos de red que se implementa.

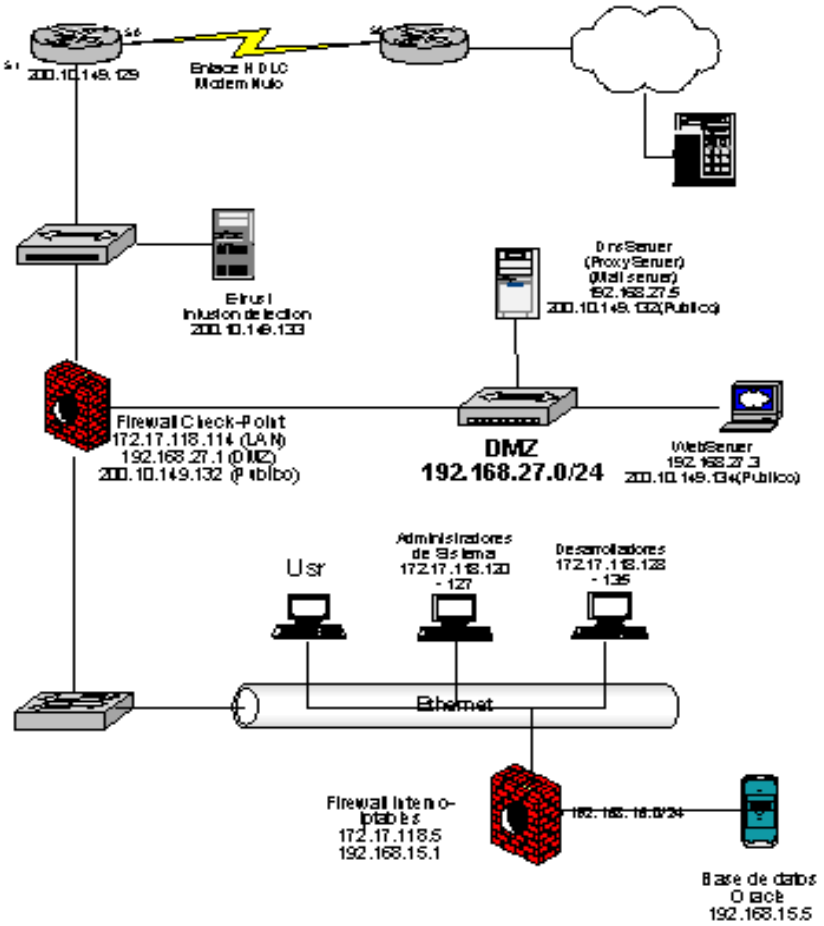


Figura 1 Esquema de Laboratorio

2.2 Diseño de Sistema

La arquitectura del sistema a implementar será Cliente/Servidor, esto significa que el usuario de Internet interactúa con una página web que a su vez se comunica con un servidor web, procesando las transacciones y peticiones del usuario. El sitio será accesible utilizando un navegador de Internet: Internet Explorer o Netscape.

El servidor web maneja los requerimientos del cliente mediante sesiones que permanecen activas en el servidor mientras el usuario esté navegando en el sitio. El servidor web interpreta los requerimientos del usuario y direcciona éstas peticiones a la base de datos, o viceversa; desde la base de datos hacia el cliente.

A continuación se muestra el diagrama transaccional que describe las funcionalidades del sistema a implementar

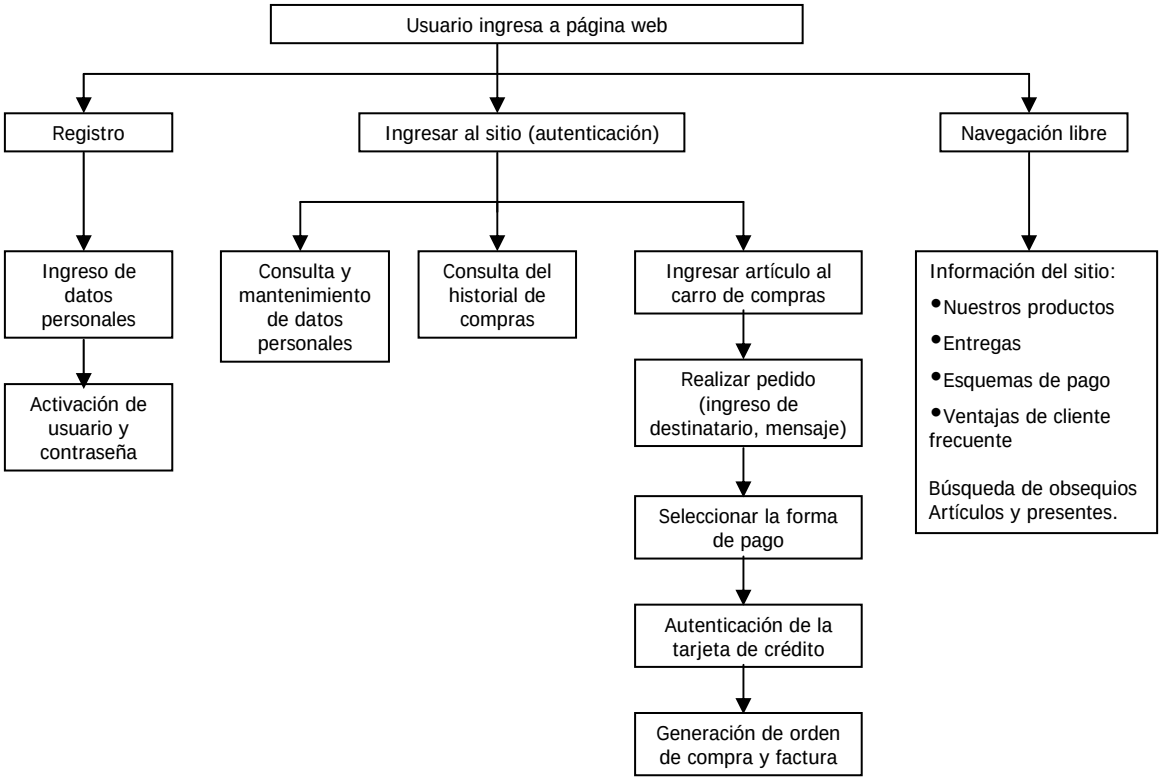


Figura 2 Transaccionalidad del sitio.

3. Implementación

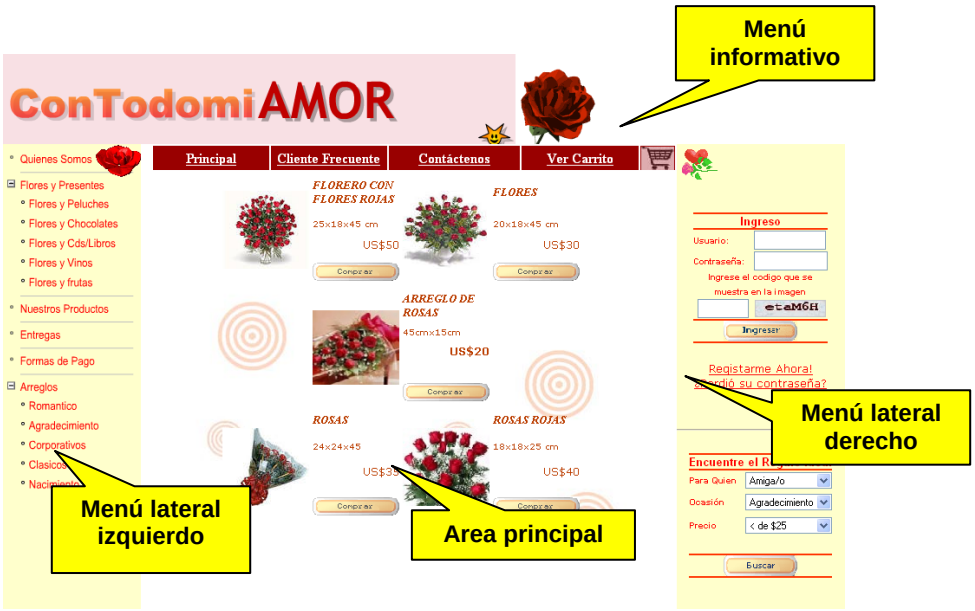
3.1. Implementación de servidores.

Para la implementación de los servicios y herramientas de seguridad se utilizo:

- Firewall Externo: Listas de acceso del ruteador de Internet
- Firewall Principal: Ckeck Point Next Generation
- Firewall Interno: Iptables Linux.
- Detector de Intrusos: E-Trust 1.5
- Bases de Datos: Oracle 9i bajo Linux
- Servidor de aplicación: Apache con páginas desarrollada en Php.

3.2. Implementación del sitio.

El sitio está implementado con cuatro frames que contiene todas las funcionalidades del sitio. Estos frames son: el “menú lateral izquierdo”, el “menú informativo”, el área principal y el “menú lateral derecho”.



El “Menú lateral izquierdo” muestra en la parte central los arreglos dependiendo de la categoría que se elija, también contiene ciertas opciones informativas como son: “Nuestros productos”, “Entregas”, “Formas de pago” y “Quiénes somos”.

El “Menú informativo” se encuentra ubicado en la parte superior central del sitio, tiene cuatro opciones que son: “Principal” el cual muestra la animación principal del sitio, la opción “Cliente frecuente” que describe la ventaja de ser cliente de nuestro sitio; la opción “Contáctenos” que permite enviar correos al administrador de la página web y la opción “Ver carrito” que permite mostrar los ítems que se ha ido agregando al carrito de compras.

El “Menú lateral derecho” esta dividido en tres funcionalidades: el área de “Ingreso de Clientes”, la opción de registrarse en el sistema y el área de “Criterios de búsqueda” para elegir un regalo de acuerdo a la ocasión.

En el área principal se mostrará los distintos arreglos que se pueden comprar, también se mostrará el carrito de compras, el resumen de la orden de compra, el detalle de los artículos, los datos de la tarjeta de pago y el resumen de factura que aparece cuando se finaliza la compra.

CONCLUSIONES

- En base al esquema de red desarrollado en el proyecto de graduación, se puede concluir que un esquema seguro debe ser implantado utilizando herramientas de bloqueo y detección en el segmento que enlaza la red objetivo con el exterior.

- En la opinión de los Autores, la primera regla para evitar ataques a sitios web es adoptar una actitud preventiva; es decir bloqueando los potenciales puntos de amenazas, tanto a nivel externo e interno de la organización.

- Se ha demostrado que mediante el uso de herramientas *"open-source"* (implantado en el firewall interno – servidor de base de datos), además de ofrecer un bajo costo en términos económicos es posible implementar esquemas confiables y seguros.

- Mediante la implementación de *"touring numbers"* incorporados a los esquemas de autenticación de usuarios, se concluye que se puede incrementar el nivel de seguridad actual en el Ecuador, dado que este mecanismo no ha sido adoptado por los sitios web locales.

- Considerando la realidad ecuatoriana respecto a medidas de protección ante ataques externos, es criterio de los Autores que la incorporación de sistemas de detección de intrusos aporta significativamente a incrementar la seguridad dado que apoya a los sistemas tradicionales basados en firewalls.

- Se concluye que una alternativa muy eficiente para asegurar la confidencialidad de la información que viaja por Internet, se logra mediante el uso de sesiones SSL; dado que su implementación no es compleja en términos tecnológicos.

- La página desarrollada implementa una interfaz amigable y fácil de usar, permitiendo al cliente varias opciones para escoger el regalo ideal para su ser querido y una forma de pago que brinda seguridad al cliente.

- A lo largo del proyecto se hace énfasis del peligro que ocasiona sistemas no correctamente auditados y actualizados, también de las vulnerabilidades existentes y las medidas a tomar para prevenirlos, con lo cual se espera lograr fomentar una cultura de seguridad tanto en los administradores de red como a nivel gerencial.

- Finalmente se concluye que en el diseño e implementación de una red no solo es importante la funcionalidad y rapidez de la misma, sino también la seguridad y respuesta inmediata ante sucesos inesperados a través de sistemas de contingencias.

REFERENCIAS

a) J. Pintag, W. Ramirez, S. Aguirre, "Desarrollo de un sitio seguro de e-commerce dedicado a la venta de arreglo florales y regalos especiales para cualquier ocasión" (Tesis de Ingeniería, Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral, 2005)
b) "Network Security Essentials Aplication and Standars" - William Stallings – 1999 Editorial: Prentice Hall
c) E-trust Intrusion Detection - Manual de Referencia- Compùters Associates
d) Tanenbaum Andrew (1997). Redes de Computadoras. México:Prentice Hall
e) Check Point Software Technologies Ltd (2001). Getting Started Guide.
f) Redwood City: Check Point Software Technologies Ltd.
g) Cisco Systems (2000). Cisco Certified Network Associate Curriculum
h) Océano (1997). Diccionario Enciclopédico Océano uno Color. España:

i) Litografía Roses S.A.
j) “Hackers 2 Secretos y soluciones para la seguridad de redes” – Joel Scambray, Stuart McClure,George Kurtz – 2001 Editorial McGraw-Hill.
k) www.answers.com
l) www.honeynet.org
m) www.cert.org
n) www.cyberpirata.org
o) www.retronet.com.ar
p) www.redhat.com
q) www.insecure.org
r) es.wikipedia.org
s) es.tldp.org
t) www.dtic.ua.es
u) www.novell.com/es-es/linux/suse/
v) fedora.redhat.com
w) microlug.linux.net.uy
x) usuarios.lycos.es
y) microlug.linux.net.uy