Módulo de políticas de seguridad y privacidad para la realización de transacciones de comercio electrónico

Trabajo de Grado

ERWIN ARNOLDO DAZA RENDÓN
FREDDY MINA GRUESO

Director: Ing. ROBERTO CARLOS NARANJO CUERVO

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Grupo de I+D en Tecnologías de la Información
Línea de Tecnologías Internet
Popayán, Junio de 2009

Nota de Aceptación

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma de Jurado

_____

Firma de Jurado

Popayán, 16 de junio de 2009

AGRADECIMIENTOS

A Dios, quién nos iluminó, guió, acompañó durante el desarrollo de nuestra investigación y por darnos la oportunidad de vivir y disfrutar de las grandes maravillas que ha creado, entre esas maravillas el poder adquirir día a día conocimientos que nos hacen crecer personal y profesionalmente.

A la Universidad del Cauca, institución que nos formó como personas brindándonos la posibilidad, a través del Programa de Ingeniería de Sistemas, de realizar nuestros estudios de pregrado y de la cual siempre hemos recibido apoyo.

Por el apoyo que recibimos en el desarrollo del presente trabajo de investigación, queremos expresar nuestros agradecimientos a las siguientes personas:

ROBERTO CARLOS NARANJO, Ingeniero de sistemas, director del trabajo de investigación, por su apoyo constante e incondicional durante el desarrollo del proyecto.

Nuestros amigos y compañeros que siempre estuvieron brindándonos su apoyo y animándonos para salir siempre adelante.

En especial a nuestros padres, hermanos y demás familiares que nos ofrecieron todo su amor, comprensión y apoyo para que este proyecto pueda culminarse.

A todas las personas que finalmente de una u otra forma nos ofrecieron ayuda en el momento más oportuno.

MUCHAS GRACIAS

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Como integrantes del Grupo de I+D en Tecnologías de la Información – GTI somos consientes de las necesidades actuales que tiene nuestra sociedad en la apropiación de la Tecnología para impulsar procesos productivos y de competitividad. A causa de ello planteamos este proyecto de grado como un trabajo de investigación por medio del cual pretendemos aportar, a la región y al país, la construcción de una cultura de Comercio Electrónico basado en la seguridad de las transacciones del lado del cliente.

Actualmente en las transacciones de comercio electrónico no existe un conjunto fuerte de políticas de seguridad del lado del cliente que le permitan resguardarse de los peligros existentes en Internet, solamente se tienen sugerencias y recomendaciones para que el mismo cliente se encargue de proteger sus propios datos, razón por la cual, el presente proyecto propone desarrollar un conjunto de políticas de seguridad que contemplen la mitigación de posibles riesgos que aún no se han tenido en cuenta para la realización de transacciones electrónicas de tipo B2C. Estas políticas de seguridad estarán soportadas en una herramienta software que se encargará de automatizarlas y servirá de complemento a los actuales mecanismos de seguridad utilizados para las transacciones comerciales en Internet, tales como técnicas de cifrado, algoritmos, protocolos, entre otros.

PLANTEAMIENTO DEL PROBLEMA

Con el desarrollo tecnológico reciente y el gran auge en el uso de Internet se está produciendo una revolución en la actividad económica global con un impacto sin precedentes en todos los sectores productivos, haciendo de la red de redes un medio atractivo y una fuente de oportunidades hacia la cual están migrando las nuevas ideas de negocios y las ya existentes, brindando nuevas formas de realizar operaciones, reduciendo costo e impactando a un número mayor de personas entre otras cosas.

Según un estudio realizado de forma exclusiva por América Economía Intelligence (AEI) para Visa internacional, se encontró que durante 2005 las ventas a través de Internet superaron los 4.300 millones de dólares en toda América Latina. Destacan los saltos ocurridos en algunos de los mercados más importantes, entre ellos, Venezuela (185%), México (104%), Chile (100%) y Brasil (43%). Cifras de Visa Internacional, que pronostican que el comercio electrónico crecerá regionalmente a tasas de 40% anual entre 2006 y 2010[1], siempre y cuando se cumpla con los cuatro elementos centrales que impulsan el e-commerce[1] en América Latina, según AEI:

- Aumento de la penetración de Internet.
- Masificación de los medios de pagos electrónicos.

[1] E-commerce: Comercio electrónico ó comercio a través de Internet.

- Profundización de la oferta de productos y servicios online[2].
- Reducción del temor de los usuarios[3] a ser víctimas de un fraude o que sus datos personales sean mal utilizados[1].

Además, en una encuesta llevada a cabo por Information Technology Association of America (ITAA) y Ernst & Young, se refleja que la barrera más importante que actúa de freno a la expansión de la actividad comercial en Internet es la falta de confianza (señalada por el 62% de los encuestados). Esta desconfianza hacia las nuevas tecnologías se articula en torno a tres temores fundamentales[2]:

- La privacidad (60%), que los usuarios finales sienten amenazada, en la medida en que desconocen hasta qué punto serán tratados los datos personales que suministran a un servidor de comercio electrónico[4]. ¿Quién le asegura al comprador que sus datos no se almacenarán a la ligera, siendo accesibles fácilmente por un hacker[5] o un empleado desleal? ¿Cómo saber que no se facilitan a terceros?

- La autenticación (56%), que inquieta a los usuarios, quienes dudan de sí la persona con la que se comunican es verdaderamente quien dice ser. Todavía la gente tiene la cultura Face To Face (compra cara a cara), ¿Cómo asegurarse que se está comprando en un sitio virtual real y no en una imitación fiel?

- La seguridad global (56%), que preocupa a los usuarios, pues temen que la tecnología no sea suficientemente robusta para protegerles frente a ataques y apropiaciones indebidas de información confidencial, especialmente en lo que respecta a los medios de pago. Es interesante el hecho de que en toda actividad de compra lo que más sigue preocupando es la operación de pago, es decir, el momento en el que el comprador se enfrenta a la ventana donde ha introducido su número de tarjeta de crédito y duda a la hora de pulsar el botón de Enviar ¿Me timarán?, ¿Seré víctima de un fraude?, se pregunta el usuario en el último momento.

La seguridad, hasta ahora, nunca ha sido uno de los principales puntos a la hora de tener en cuenta en el desarrollo y la evolución de Internet. Parece que este detalle tiende a cambiar, ya que la seguridad en el comercio electrónico busca la seguridad de los datos de sus usuarios[3]. A causa de ello surge la siguiente pregunta: ¿Cómo proveer un mecanismo que verifique el grado de seguridad de la transacción electrónica a la que se enfrenta el usuario y que contribuya a incrementar su nivel de confianza?

Para resolver la anterior inquietud, se plantea la implementación de un **"Módulo de políticas de seguridad y privacidad para la realización de transacciones de comercio electrónico**", que automatizará las políticas que se propongan en este

[2] Productos y servicios online: Servicios ofrecidos en Internet.

[3] Los usuarios son las personas que utilizan Internet, también se les denomina Cliente Web.

[4] Los usuarios finales desconocen la forma en la cual son tratados sus datos. No saben si hay confidencialidad en el tratamiento de sus datos.

[5] Persona con alto grado de conocimientos relacionados con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red, etc.

proyecto, para reducir los riesgos asociados a las transacciones electrónicas y a los que están expuestos los usuarios.

La implementación de las políticas será integrada en un navegador Web de código libre[6], brindando un mayor nivel de confianza al usuario al mantenerlo informado del grado de seguridad del proceso de la transacción electrónica que realice en un sitio Web que ofrezca productos y servicios. Además, el módulo software, de forma automática, garantizará la verificación de cada uno de los elementos necesarios para ofrecer seguridad en el intercambio de datos en transacciones electrónicas.

La anterior propuesta busca mejorar los niveles de confianza a la hora de realizar transacciones en línea motivando a los clientes a incrementar el uso de medios de pago electrónicos, lo cual impactará significativamente el desarrollo del Comercio Electrónico.

OBJETIVO GENERAL DEL PROYECTO

Proponer[7] y automatizar un conjunto de políticas y recomendaciones de seguridad, mediante la construcción de un módulo software que se podrá integrar a un navegador de código libre, que contribuya a disminuir los riesgos a los que está expuesto el cliente en la realización de transacciones de comercio electrónico B2C a través de tarjetas de crédito y débito.

OBJETIVOS ESPECÍFICOS

- Generar un conjunto de políticas y recomendaciones de seguridad, que disminuyan los riesgos identificados en transacciones electrónicas, que sirvan de apoyo y protección a los usuarios en la realización de pagos con tarjetas de crédito y débito.

- Diseñar y construir un módulo software, basándose en la metodología de desarrollo de software UP y en técnicas de Ingeniería del Software, que automatice el conjunto de políticas de seguridad generadas.

- Integrar el módulo software a un navegador Web de código libre para probar y validar las políticas de seguridad propuestas, así como el software construido.

METODOLOGÍA

Para el desarrollo del presente proyecto, en cuanto a la parte de investigación, se siguió inicialmente la metodología propuesta en el Modelo para la Investigación Científica, expuesta en el libro Modelo Integral para el Profesional en Ingeniería[4]:

[6] Código libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

[7] Proponer ante la comunidad académica el conjunto de políticas.

Este modelo presenta un conjunto de 4 Etapas las cuales a su vez se componen de una serie de Fases las cuales se detallan a continuación:

Etapa 1 (Definición): que permite efectuar el inicio del proceso investigativo escogiendo el objeto de investigación y el área de conocimiento. Para esto se debe: seleccionar el área de la temática que implica la elección de un campo de trabajo y del objeto[8] de investigación que determina el problema a solucionar.
En esta etapa se realiza un estudio preliminar sobre el estado del arte del proyecto para determinar el objeto de investigación a seguir.

Etapa 2 (Formulación): cuyo propósito es la organización del proyecto indicando claramente: el problema existente que se quiere abordar, delimitación de la investigación, elaboración del soporte teórico y la estrategia a seguir para atacar el problema planteado (diseño bibliográfico) [9].
Durante esta etapa de investigación mediante observación y exploración de información sobre riesgos y políticas de seguridad existentes en transacciones de comercio electrónico, se obtendrán los datos requeridos y se identificarán las falencias presentes en este tipo de transacciones.

Etapa 3 (Ejecución) cuyo propósito es definir técnicas de recolección de datos, elaborar instrumentos para su recolección, recolectarlos y procesarlos, para finalmente clasificarlos y ordenarlos.

Etapa 4 (Síntesis) cuyo propósito es obtener una nueva elaboración teórica que refleje el conocimiento generado como resultado del proceso investigativo. Para esto se debe: analizar y sintetizar la información, finalmente presentar los resultados obtenidos.

Para analizar, sintetizar y obtener resultados con respecto a la información recolectada se escogió la metodología de análisis de riesgos Magerit[5], la cual permite encontrar los requerimientos de seguridad de la organización o proceso identificando los activos mas relevantes para esta. La relevancia de estos la da su nivel de exposición al riesgo el cual se mide por medio del riesgo residual que resulta al aplicar las salvaguardas del caso. La metodología requiere que se sigan los siguientes procesos:

Proceso de Análisis de Riesgos: que presenta las siguientes actividades:

- **La Estructuración del Proyecto de Análisis de Riesgos**: su planificación (objetivos y su alcance), definición de activos y su clasificación.

- **Valoración del Riesgo**: En esta los activos identificados se clasifican por capas, se valoran por frecuencia de uso, se dimensionan, se identifican las dependencias, sus amenazas y vulnerabilidades presentes.

- **Estimación del Estado del Riesgo**: en este se debe calcular el riesgo, el cual incluye; encontrar el impacto económico causado por la materialización de una

[8] Objeto de Investigación hace referencia al problema de conocimiento que se quiere abordar.

[9] Diseño bibliográfico: Se trabaja fundamentalmente con datos secundarios, es decir, datos obtenidos, elaborados y procesados por terceros en el desarrollo de sus investigaciones.

amenaza sobre un activo y la probabilidad de ocurrencia e interpretar los resultados.

Proceso de Gestión de los Riesgo: el cual incluye seleccionar las salvaguardas necesarias y determinar la calidad necesaria para dichas salvaguardas.

El porqué realizar un análisis de riesgos viene de la mano de algunas guías como la ISO 17799 [6] y el RFC2196[7], las cuales tienen orientaciones para la creación de políticas de seguridad. Gracias a estas guías se pueden seleccionar los controles adecuados para mitigar los riesgos; estos controles se pueden adoptar de la misma guía, otros estándares ó se pueden crear siguiendo sus recomendaciones. Entre los controles implementados más importantes, se tienen el uso de políticas de seguridad.

En cuanto a la creación del diseño de las políticas se optó por seguir la metodología sugerida por la Universidad Nacional de Colombia [8] en su guía para la elaboración de políticas, la cual es un texto traducido y adaptado del libro "The Security Policy Life Cicle: Functions and Responsabilities".

Para la creación del componente software, como metodología de desarrollo de software se seleccionó el Proceso Unificado de desarrollo de software (UP) [9]de la mano con la guía expuesta en el libro de Doug Turner & Ian Oeschger "*Creating XPCOM Components*" [10]útil a la hora de construir componentes XPCOM.

RESULTADOS ESPERADOS DEL PROYECTO

Con el desarrollo del presente proyecto se espera obtener un conjunto de políticas y recomendaciones de seguridad y una herramienta software que permita automatizarlas. La herramienta software con la verificación de las políticas implementadas brindará información respecto al grado de seguridad, que el sitio Web ofrece, para los datos del usuario en el momento en que este se dispone a realizar una transacción electrónica.

RESUMEN DE LOS CAPÍTULOS QUE COMPONEN LA MONOGRAFÍA

Esta monografía de grado corresponde al proyecto denominado "*Módulo de políticas de seguridad y privacidad para la realización de transacciones de comercio electrónico"* y está organizada en 6 capítulos los cuales se exponen a continuación:

Capítulo 1: En este capítulo se muestran las bases conceptuales que se utilizaron para la consecución de este proyecto.

Capítulo 2: Se identificarán elementos y componentes[10] que intervienen en las transacciones electrónicas B2C. Además, se indicarán que problemas y que amenazas se encuentran presentes en cada uno de los componentes. Este capítulo tiene un estudio

[10] Componentes hace referencia a elementos presentes en transacciones electrónicas B2C, tales como navegadores, antivirus, protocolos de conexión, entre otros.

a fondo sobre los riegos y políticas de seguridad, en el cual se identifican las falencias en las políticas de seguridad actuales y los riesgos que no se hayan tenido en cuenta en transacciones electrónicas B2C, y se empezará a abordar el problema planteado.

Capítulo 3: Este capítulo analiza y sintetiza la información obtenida y en el se generará un conjunto de políticas de seguridad para transacciones de comercio electrónico B2C. Este conjunto de políticas obtenidas se propondrán ante la comunidad académica.

Capítulo 4: Este capítulo expone la construcción del módulo software que se integrará a un navegador Web el cual automatizará las políticas propuestas en el capítulo anterior. En este capítulo se describirá en forma detallada el proceso de análisis y diseño del módulo, incluyendo los requisitos funcionales y no funcionales del software. En cuanto a la implementación del módulo se realizará una explicación detallada de los elementos utilizados para esta etapa en el Anexo D y E correspondiente a la implementación.

Capítulo 5: Este capítulo muestra las pruebas realizadas al software construido y se plasman los resultados obtenidos.

Capítulo 6: En este capítulo final toda la información referente a experiencias obtenidas, problemas presentados y sus respectivas soluciones, se describen como un conjunto de conclusiones y recomendaciones.

1 MARCO TEÓRICO

En este capítulo se describen los conceptos básicos referentes a tecnologías y temáticas relacionadas con el desarrollo de este proyecto, así como las bases conceptuales necesarias para la consecución del mismo. Se tratarán temas como sistemas de pagos electrónicos, mecanismos para proveer seguridad en transacciones de comercio electrónico, cifrado, certificados digitales, entre otros.

Estos conceptos se relacionan con la seguridad en el comercio electrónico y ayudarán al lector a adquirir un mayor grado de comprensión del problema a tratar.

1.1 CONCEPTOS FUNDAMENTALES

1.1.1 COMERCIO ELECTRÓNICO

Según Jeffrey, R. & Bernard, J. El comercio electrónico se define como: "*Intercambios mediados por la tecnología entre diversas partes (individuos, organizaciones o ambos), así como las actividades electrónicas y no electrónicas dentro y entre organizaciones que facilitan esos intercambios.*" [11].

El comercio electrónico se puede clasificar en varias categorías, pero en este apartado solamente se expondrán las más relevantes:

1.1.1.1 Comercio Electrónico Business to Consumer (B2C)

Este tipo de comercio electrónico es aquel comercio electrónico negocio a consumidor. Aquí la empresa realiza funciones de mercadeo, promoción, publicación de información y catálogos de productos o servicios dirigidos al usuario final [12].

1.1.1.2 Comercio Electrónico Business to Business (B2B)

El comercio digital negocio a negocio permite a dos empresas realizar transacciones seguras, las cuales intercambian información directamente entre sus sistemas computacionales.

Desde la perspectiva de las organizaciones, el comercio digital negocio a negocio facilita las siguientes actividades del negocio [12].

- *Administración de los suministros*: para reducir los tiempos y costos de procesamientos de compras.
- *Administración del inventario:* para reducir los tiempos de orden, embarque y distribución.
- *Administración de la distribución*: para facilitar el envío de documentación de embarque como son notas de carga, órdenes de compra y manifiestos de reclamo entre otros, permitiendo mayor precisión en la información presentada.
- *Administración de los canales de distribución*: para diseminar la información de forma rápida y segura acera de especificaciones técnicas o de pago.

- *Administración del pago*: para el envío o recepción de pagos electrónicos entre los proveedores o distribuidores incrementando la velocidad y reducción de errores al realizar los pagos de facturas.

1.1.2 SISTEMAS DE PAGOS ELECTRÓNICOS

En la actualidad existen varios medios electrónicos que permiten la realización de pagos a través de Internet, cada uno con diferentes características que permiten brindar distintos niveles de seguridad a los usuarios, algunos de ellos se presentan a continuación:

1.1.2.1 Tarjetas Inteligentes

La primera tarjeta inteligente se desarrolló en 1974, por Roland Moreno. Una tarjeta inteligente es una tarjeta que tiene incluido un microprocesador y un chip de memoria, o sólo un chip de memoria. El microchip es capaz de controlar las operaciones efectuadas, pero requiere un equipo terminal apropiado para la computadora. Cuando se realice una compra, el dinero sería transferido desde la tarjeta del comprador a la del vendedor; incluso a cualquier otra tarjeta si se deseará realizar una simple transferencia de dinero entre ambas [13].

1.1.2.2 Tarjetas de Crédito y Débito

Son utilizadas para realizar pagos sin necesidad de efectivo y hoy en día son uno de los medios más utilizados para realizar este tipo de transacciones sobre Internet [14]. Entre las partes involucradas en estas transacciones tenemos: el cliente, el comerciante, el banco del cliente, el banco del comerciante y la red interbancaria.

Entre los tipos de transacción que se efectúan en la Web con tarjeta de crédito o débito tenemos:

- Fuera de línea: aquí el cliente hace una orden de compra dentro de un sitio Web y luego el comerciante le llama vía telefónica, confirma la orden de compra y le solicita los datos de la tarjeta.

- En línea: aquí el cliente envía el número de la tarjeta al comerciante a través de Internet en el mismo instante en el cual se realiza la transacción.

En el método fuera de línea el problema que se tiene se debe a que la línea telefónica pueda estar interceptada y existe el riesgo que los datos confidenciales del usuario como los de la tarjeta sean robados.

Para el método en línea se debe tener en cuenta que el método use encriptación de los datos, ya que gracias a esto se hace posible que dicho método sea el más confiable.

Pagar con tarjetas débito en Internet se hace más peligroso para los clientes, ya que el pago con esta se debita en el momento de realizar la compra caso contario a las tarjetas

de crédito. Además, en cuanto a resolución de disputas cuando se cometen fraudes con las tarjetas de crédito es responsabilidad del comerciante con el cual se realizo la transacción, por este motivo se debe verificar la identidad del mismo antes de realizar cualquier transacción. En cuanto a responsabilidades con tarjetas débito, la perdida de la misma o de claves, hace que las consecuencias de la perdida recaigan sobre el titular de la tarjeta.

En conclusión, la forma más segura para el cliente a la hora de realizar transacciones con tarjetas débito o crédito es la tarjeta crédito; esto debido a la forma como se resuelven las disputas y el tiempo transcurrido antes de debitar la compra. Además, se debe tener en cuenta que para realizar una transacción con estos medios, primero hay que verificar la identidad del sitio con el cual se va a realizar la transacción y segundo que los datos que se van a enviar, los cuales son sensibles, deben estar cifrados y borrados al final la transacción [28].

1.1.3 MECANISMOS PARA PROVEER SEGURIDAD EN TRANSACCIONES ELECTRÓNICAS

1.1.3.1 Protocolos estándar de seguridad

Existen dos protocolos estándar de seguridad: SET y SSL, sistemas que cifran los datos del usuario para que nadie pueda acceder a ellos [15][16]. Estos protocolos se exponen a continuación:

1.1.3.1.1 SET (Secure Electronic Transaction)

Es un conjunto de normas de seguridad que adjunta un certificado al pago que se realiza mediante tarjeta de crédito. Este protocolo fue diseñado con la intención de asegurar y autenticar la identidad de las personas que participan en las transacciones efectuadas a través de cualquier red en línea.

El objetivo primordial de SET es mantener la confidencialidad de la información intercambiada en una transacción, así como garantizar la integridad del mensaje y la identidad de los participantes, con objeto de evitar los fraudes, falsificaciones y uso ilegitimo de tarjetas de crédito en Internet.

SET proporciona los medios para que consumidores y comerciantes se identifiquen entre ellos antes de la realización de la transacción. Su funcionamiento se basa en la utilización de certificados digitales y de la encriptación de claves públicas para proteger la información financiera de los participantes [15].

Inconvenientes del protocolo SET

- SET aún no esta completamente implantado en Internet debido, en primer lugar, a la necesidad de utilizar un software especial (tanto para compradores como para comerciantes) cuya distribución y comercialización se está desarrollando muy lentamente.

- El funcionamiento del SET resulta complejo y confuso para los usuarios.
- Es controlado por un consorcio que impone sus propias normas y por lo cual muchos comerciantes prefieren otras soluciones de pago [16].

- Es utilizado solo para transacciones con tarjeta de crédito.

- No es adecuado para pagos de poco valor.

1.1.3.1.2 SSL (Secure Socket Layer)

Es una tecnología desarrollada por Netscape en 1994 junto con su primer navegador, para asegurar la privacidad y fiabilidad de las comunicaciones entre dos aplicaciones. Utiliza un sistema de cifrado asimétrico basado en claves pública/privada para negociar una clave que luego se utilizará para establecer una comunicación basada en cifrado simétrico. (Para profundizar más en el tema de cifrado, ver sección 1.1.3.4 de esta monografía).

La seguridad de SSL actualmente proporciona servicios de cifrado de datos, servidor de autenticación, integridad de mensaje y autenticación de cliente para una conexión de TCP/IP. A continuación, se presenta un conjunto de características presentes en este protocolo:

- Cifrado de datos: la información transferida se cifra utilizando un algoritmo de clave secreta, capaz de cifrar grandes volúmenes de información en muy poco tiempo, por lo que resultará ininteligible en manos de un atacante, garantizando así la confidencialidad.

- Autenticación de servidores: el usuario puede asegurarse de la identidad del servidor al que se conecta y al que posiblemente envíe información personal confidencial.

- Integridad de mensajes: se impide que pasen inadvertidas modificaciones intencionadas o accidentales en la información mientras viaja por Internet.

- Opcionalmente, autenticación de cliente: permite al servidor conocer la identidad del usuario, con el fin de decidir si se puede acceder a ciertas áreas protegidas. En este caso, el cliente debe tener instalado un certificado en su ordenador o en una tarjeta inteligente, que le permitirá autenticarse ante el servidor Web. Se evitan así ataques comunes de captación de contraseñas mediante el uso de sniffers[11] [17] o la ejecución de reventadores de contraseñas.

Un sitio puede identificarse como seguro si su dirección URL comienza con **https://** en lugar de **http://**, o si en el navegador aparece algún indicador de sitio certificado (Netscape muestra una llave  , mientras que en Internet Explorer de Microsoft o Mozilla Firefox muestran un candado  , en la parte inferior izquierda de la ventana).

[11] Sniffer: Analizadores de protocolos. Programa que escanea la información que viaja a través de la red.

En cuanto al funcionamiento, SSL utiliza una capa ubicada entre el protocolo de hipertexto (http) y el protocolo de transporte (TCP); esto es entre los niveles de transporte y aplicación del protocolo TCP/IP, (ver Figura 1.1), permitiéndole dar seguridad a todas las aplicaciones que se encuentran entre estas dos capas [18].

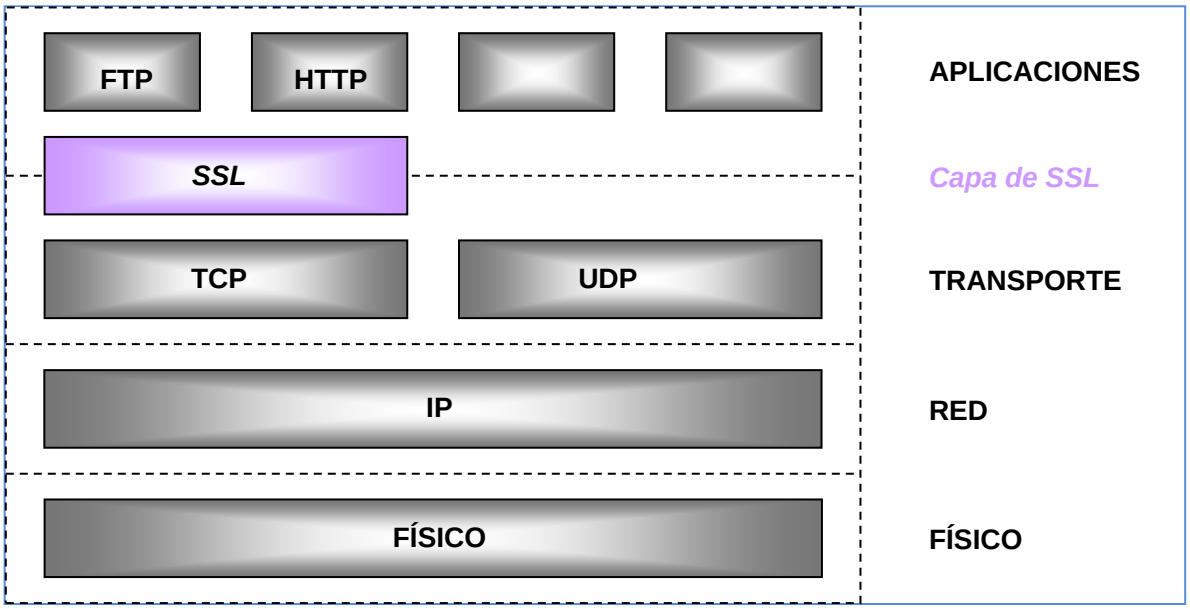

Figura 1.1 Modelo TCP/IP

SSL utiliza dos tecnologías de cifrado para brindar todos los servicios de seguridad necesarios en una transacción: la criptografía de clave pública[12] [19] (asimétrica) y la criptografía de clave secreta[13] [19] (simétrica). Para el intercambio de los datos, utiliza algoritmos de cifrado simétrico como: DES (Data Encryption Standar), Triple DES, RC2 (Rivest's Cipher), RC4 o IDEA (Internacional Data Encription Algorithm) [19]. Para la autenticación y para el cifrado de la clave de sesión, usa un algoritmo de cifrado de clave pública. La clave de sesión es la que se utiliza para cifrar los datos durante una transacción al haber establecido un canal seguro

Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea descifrada no sirva para descifrar datos de futuras transacciones. El nivel de seguridad proporcionado por los algoritmos de cifrado, utilizados por SSL, lo brinda la cantidad de bits utilizados para generar las claves.

Inconvenientes de SSL

- Solo garantiza la integridad y confidencialidad de los datos cuando están en transito por la red.

[12] Para esta tecnología, cada usuario posee un par de claves, una privada y otra pública. Esta última es la que utiliza otro usuario para enviar información de forma segura y la privada es utilizada por su dueño para descifrar esta información.
[13] En esta tecnología de cifrado el emisor y receptor comparten una clave secreta para cifrar y descifrar los mensajes.

- Los datos de los usuarios se cifran con la llave pública del comerciante permitiendo que este tenga acceso a información tal como número de tarjetas de crédito e información que sólo debería tener el banco.

- No permite verificar la validez de las tarjetas de crédito o debito.

- No posee mecanismos para garantizar el no repudio y por ende ninguna de las partes se ve comprometida a hacerse cargo de la transacción [16].

1.1.3.2 Certificado Digital

Un certificado digital o certificado electrónico es un bloque de caracteres que acompaña a un documento o archivo acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor [20]. En la Figura 1.2, se puede apreciar el aspecto de un Certificado Digital:

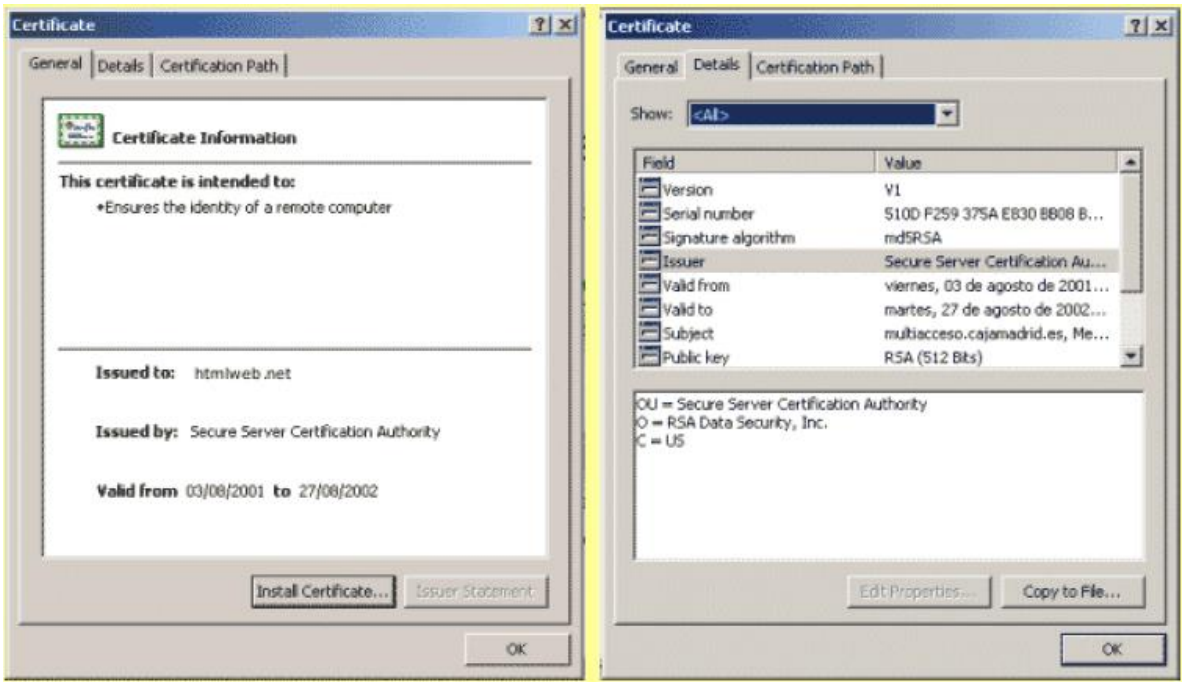

Figura 1.2 Ejemplo de Certificado Digital

1.1.3.3 Certificados Extended Validation

Son certificados SSL con validación ampliada. Estos permiten la protección de los usuarios frente a actividades fraudulentas gracias a una verificación, a través de terceros, de la autenticación de los sitios Web.

Exploradores como Internet Explorer 7 y Mozilla Firefox versión 3.0.8 ofrecen una referencia visual (barra de direcciones de color verde en el navegador Web), cuando las páginas Web presentan Certificados con Extended Validation [21]. La barra de direcciones URL de los dos exploradores también muestra el nombre de la organización registrada y el nombre del proveedor de SSL con Extended Validation.

1.1.3.4 Cifrado

El cifrado es posible gracias al uso de la criptografía. Esta técnica se ha utilizado por muchos años para encriptar la información. La criptografía viene del griego *Kriptos*, "escondido", y *graphos*, "escritura". Es el arte de enmascarar los mensajes con signos convencionales, que sólo cobran sentido a la luz de una clave secreta. La seguridad de un mensaje no depende del método (algoritmo criptográfico) utilizado para cifrar la información, sino de la clave utilizada para realizar dicho proceso (longitud de la clave medida en bits y caracteres que puede incluir) [22].

Clasificación según el tipo de clave

Según el tipo de clave utilizada para cifrar la información la criptografía se puede clasificar en:

- **Criptografía simétrica:** En este tipo de criptografía se utiliza la misma clave para cifrar y descifrar la información, ver Figura 1.3:

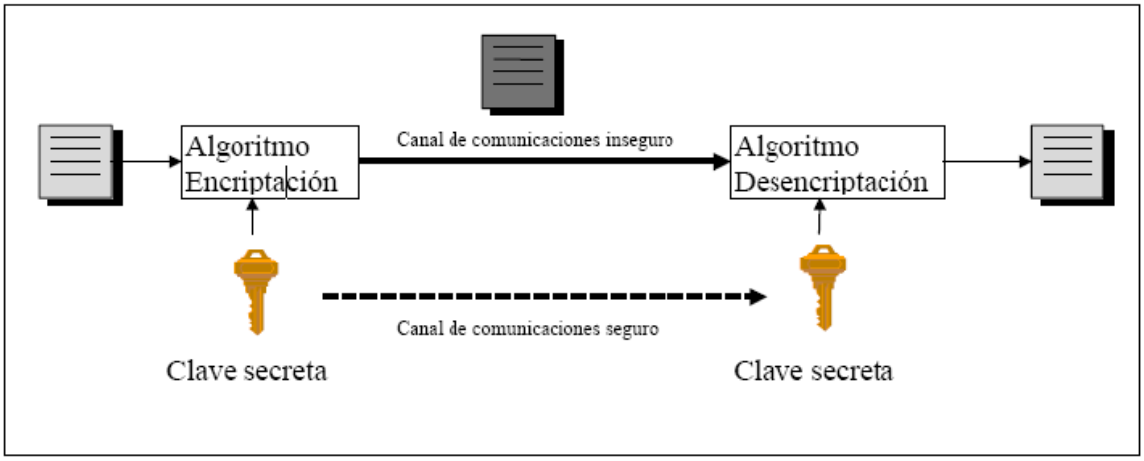

Figura 1.3 Criptografía Simétrica

El gran inconveniente es que toda la seguridad está basada en la clave secreta y la distribución de la misma debe garantizar que se entregan las llaves a los usuarios autorizados. Este último inconveniente se resuelve hoy en día mediante sistemas asimétricos montados únicamente para la transmisión de claves. Este tipo de criptosistema garantiza la confidencialidad de la información, pero no garantiza la autenticación ni la firma digital de mensajes [23].

- **Criptografía de clave pública o asimétrica:** En este tipo de criptosistema, ver Figura 1.4, se utilizan dos claves, una se hace pública y la otra privada, que es conocida sólo por un dueño y permite recuperar los mensajes cifrados con su clave pública [22].

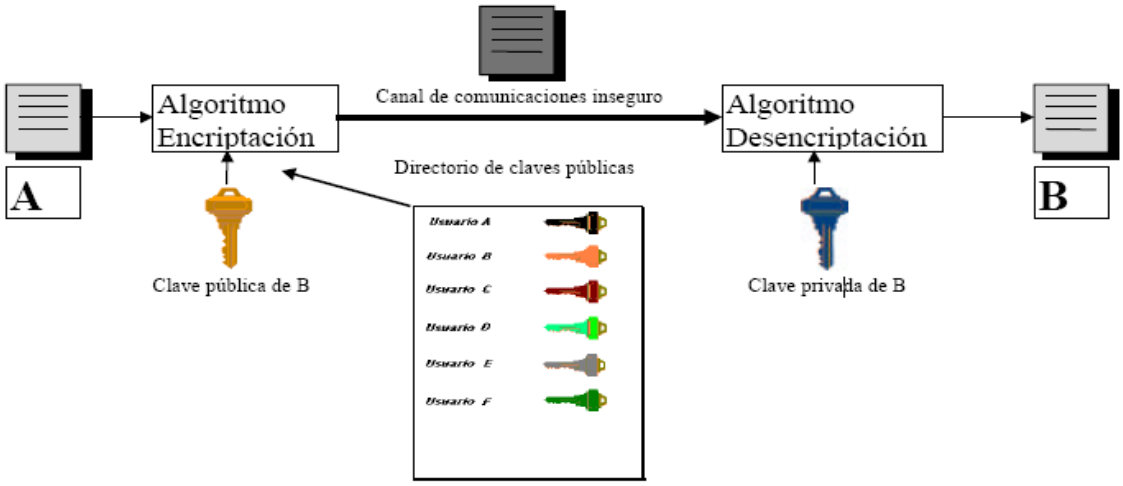

Figura 1.4 Criptografía Asimétrica

A diferencia de la criptografía simétrica, esta permite confidencialidad, integridad, autenticación y firmado digital del mensaje.

Los sistemas criptográficos asimétricos utilizan diferentes algoritmos criptográficos los cuales se simplifican en la Tabla 1.1:

Algoritmo	Tamaño de la clave en Bits
DES	56
TRIPLE DES	112
IDEA	128
RC2	8-1024
RC5	0-2040
BLOWFISH	43-448
SKIPJACK	80
CAST	40-128
AES	128,192 Y 356

Tabla 1.1 Algoritmos más utilizados en sistemas criptográficos asimétricos [23].

1.1.3.5 Servidores seguros

Un servidor seguro garantiza que la información que viaja entre él y el navegador del usuario vaya cifrada, de tal forma que no puede ser leída de forma legible si es interceptada en la red o ser manipulada en el peor de los casos, garantizando la confidencialidad de la información que se haya enviado.

Al conectarse a un servidor seguro, este le obliga a que se autentifique. La seguridad de estar en un servidor seguro, se obtiene mediante un certificado digital, el cual es expedido por una compañía independiente, la cual está autorizada legalmente para garantizar que un determinado servidor pertenece a una compañía determinada. A través del certificado de seguridad el usuario obtiene la confirmación de que está enviando la información al lugar correcto.

El objetivo de un servidor de este tipo es incrementar la confiabilidad y fiabilidad de las transacciones on-line y mantener en todo momento la privacidad de los datos transmitidos de servidor a cliente y viceversa [16].

1.1.3.6 Pasarelas de pago

Son las encargadas del procesamiento de las tarjetas de crédito desde Internet hacia las redes privadas de sistemas como VISA, Mastercard, American Express, etc.

La función básica de estas es evitar que la información sobre la tarjeta de crédito del comprador llegue directamente al vendedor, siendo utilizada únicamente por la entidad bancaria; al vendedor sólo se le entrega una notificación del éxito o fracaso de la transacción.

La operación de pago a través de una pasarela de pago consta de las siguientes fases [16]:

- El cliente utiliza una aplicación de comercio electrónico para elegir los productos que desea adquirir; la aplicación calcula el importe total de la compra.

- Cuando el cliente decide pagar, la aplicación de comercio electrónico le redirige al servidor seguro del banco y le indica a la pasarela de pago la cantidad total a cobrar para que procese el pedido.

- El cliente introduce el número de su tarjeta de crédito en un formulario del servidor seguro del banco (los datos viajan debidamente cifrados).

- El banco realiza una comprobación de la validez de la tarjeta de crédito y de la existencia de fondos. Si la respuesta es afirmativa, se realiza el cobro ingresando el dinero en la cuenta bancaria del vendedor.

- El servidor seguro del banco redirige al cliente de vuelta a la aplicación de comercio electrónico indicando si la operación se ha realizado o no con éxito.

En conclusión, todos los conceptos anteriormente mencionados y explicados son los principales componentes utilizados para garantizar la seguridad de los datos de los usuarios a la hora de realizar transacciones en línea. A partir de aquí será más fácil la comprensión de los capítulos posteriores, ya que se tendrá un conocimiento más amplio en cuanto a:

- Cifrado, que va de la mano con la criptografía la cual es el pilar sobre el cual se fundamenta la seguridad.
- Los tipos de algoritmos y sus fortalezas en cuanto a la cantidad de bits utilizados para cifrar los datos.
- Certificados digitales y su utilización como mecanismos para garantizar la autenticación de las partes involucradas dentro de una transacción electrónica.

1.2 PROYECTOS EXISTENTES

Existen proyectos, establecidos por organizaciones, relacionadas con la seguridad en las transacciones electrónicas, tales como:

1.2.1 Políticas de Seguridad Banco de Bogotá

El Banco de Bogotá incorpora una serie de políticas de seguridad y privacidad para sus usuarios. Las políticas de seguridad son: la certificación de la página Web, máxima encriptación de datos, protocolos de comunicación seguros, identificación de usuarios y protección de los datos. Algunos de los problemas detectados radican en la utilización de la clave de la tarjeta de crédito, como por ejemplo, para identificación del usuario, además estas políticas de seguridad se deben complementar con las políticas de privacidad las cuales son en su mayoría responsabilidad del usuario [24].

1.2.2 Norton Confidential de Symantec

Es una herramienta software que ayuda a [25]:

- Desenmascarar el phishing (suplantación de identidad) y el pharming (reorientación hacia otras páginas).
- Descubrir el crimenware (software malicioso).
- Autenticación de sitios Web.
- Proteger contraseñas.
- Estrategias de seguridad a mayor escala (integración de todos los componentes de la gama Norton de Seguridad).

Esta herramienta, según Symantec, debe ser complementada con hábitos inteligentes que ayuden a reforzar la seguridad. Entre estos hábitos se cuentan.

- Realizar sus conexiones y transacciones en sitios encriptados.
- Use sitios autenticados, para evitar digitar datos importantes en páginas falsas.
- Monitoreé constantemente el estado de sus cuentas.
- Proteja su identidad.
- Adopte nombres de usuarios y contraseñas complejas de descubrir.

Pero el gran problema radica en la utilización o puesta en práctica de estos hábitos, debido a que no se encuentran implementados en la herramienta como políticas o sugerencias y en muchos de los casos son desconocidos o no utilizados por los usuarios. Otro problema que existe es el costo de licenciamiento de las herramientas y las restricciones a la licencia, estas restricciones van desde el otorgamiento por un determinado tiempo hasta determinar el número de máquinas que pueden funcionar bajo una misma licencia.

1.2.3 Google Checkout

Es un servicio de pagos por Internet en el cual el usuario tiene que crear una cuenta para poder utilizar el servicio de transacciones. Google Checkout actúa como una pasarela de seguridad entre el comercio electrónico y el cliente. El usuario solo tiene que ingresar sus datos de tarjeta de crédito solo cuando crea su cuenta en Google Checkout, después este actúa como un intermediario en la transacción [26].

El servicio no le garantiza protección al cliente contra ataques tipo phishing ni le garantiza la autenticidad del sitio en el cual esta comprando. Además, provee al sitio los datos de la tarjeta de crédito del cliente para la compra eximiéndolo de este paso, ¡lo cual no garantiza aumento de la seguridad en la transacción sino que aumenta los riesgos para el cliente!

1.2.4 Pay Cash (Sistema de Pago Seguro y Eficiente sobre Internet)

Fue diseñado para ofrecer una fuerte seguridad y protección a los datos. Extendido para apoyar una política de anonimato flexible y seguridad en las leyes que difieren de país a país. Para proteger la seguridad y privacidad Pay Cash fue diseñado para hacer lo siguiente:

- Registros para pruebas de sabotaje.
- Protección de la privacidad: para proteger el robo de identidad.
- Políticas de anonimato flexibles. Dependiendo del país y de la legislación.

- Gama de pagos: de diferentes montos.
- Múltiples monedas.
- Escalabilidad.

A pesar de todo lo anterior el sistema de pago Pay Cash no tiene registros de manipulación de las transacciones, con lo cual, se pueden presentar problemas a la hora de demostrar transferencias de fondos o cantidades disponibles de dinero. Tampoco ofrece ninguna forma de resolver disputas entre usuarios y el sistema de pago operador [27].

Estos antecedentes incorporan mecanismos de seguridad para disminuir el riesgo en las transacciones, pero no tiene en cuenta el nivel de experiencia del usuario o el conocimiento que este pueda tener acerca de la seguridad a nivel de red, su propio equipo (computador) y la transacción en si. A su vez, los mecanismos de seguridad deben ser complementados con hábitos inteligentes que ayuden a fortalecer la seguridad y es en este punto donde se apoya el trabajo de grado a realizar, pues permitirá fortalecer la utilización de hábitos inteligentes (por parte de usuario) y permitirá la aplicación de políticas de seguridad para guiar al usuario a través de todo el proceso de la transacción.

1.2.5 PayPal

PayPal es un sistema perteneciente al sector del comercio electrónico, que permite a cualquier persona que tenga un correo electrónico transferir dinero utilizando su tarjeta de crédito de manera segura.
La seguridad de la información referente a la transacción y al dinero se basa en el protocolo SSL, el cual cifra la información hasta 128 bits de longitud.
PayPal está licenciado por el programa de seguridad Trusted, la cual es una organización sin ánimo de lucro [50].

PayPal presenta las siguientes ventajas:

- Permite pagar en línea con cualquier tarjeta de crédito.
- Es gratuito para enviar dinero.
- Es seguro y privado.
- El servicio es gratuito para el comprador.

El inconveniente de PayPal es que se queda con los datos del usuario, los datos de la transacción y con los datos financieros de la tarjeta; lo cual se puede convertir en un problema serio en caso de que se pierda la información que PayPal maneje [50].

1.2.6 Aspectos legales

En Colombia el aspecto legal referente al comercio electrónico esta dado por ley 527 de 1999. Esta ley contempla aspectos como: reglamentación en mensajes de datos, transporte de mercancías, certificados digitales, firmas digitales, entidades de certificación y el papel que desempeña la superintendencia de industria y comercio [51].

Los aspectos más importantes de esta ley son:

- Es de origen internacional.
- Garantizar la seguridad e integridad en la transmisión de mensajes de datos.
- Describe las características que debe tener un certificado digital y cómo este puede ser revocado.
- Garantizar que el transporte de mercancías adquiridas en el comercio electrónico cumplan con los requisitos de etiqueta del producto, recibo de facturación, confirmaciones de envío y recibo de la mercancía, entre otros.

2 IDENTIFICACIÓN DE AMENAZAS PARA LOS USUARIOS DE TRANSACCIONES DE COMERCIO ELECTRÓNICO B2C Y LOS COMPONENTES, RECOMENDACIONES Y POLÍTICAS DE SEGURIDAD UTILIZADOS PARA SU MITIGACIÓN

Los usuarios de transacciones B2C están sometidos a una serie de amenazas que afectan a los navegadores Web, y a través de estos a las propias computadoras de los usuarios; estas amenazas les permiten a los atacantes apropiarse de los recursos computacionales (datos, programas, recursos de red, etc.). Es importante reconocer estas amenazas y los mecanismos que actualmente se utilizan para mitigarlas, pues gracias a este reconocimiento inicial es que se puede mejorar la seguridad al navegar y al realizar transacciones en línea. También se hace necesario indagar por la existencia de políticas y/o recomendaciones que puedan existir concernientes a la realización de transacciones B2C, ya que mediante el conocimiento de estas se puede identificar las falencias y necesidades de mejorar dichas políticas y recomendaciones. A continuación se detallan estos puntos.

2.1 AMENAZAS PARA USUARIOS DE TRANSACCIONES B2C Y COMPONENTES NECESARIOS PARA MITIGARLAS.

Para un mejor entendimiento e identificación del ámbito en el que actúan las amenazas para usuarios de transacciones B2C y los mecanismos necesarios para mitigarlas, estos se abordarán desde tres perspectivas: en primer lugar, asegurar la computadora del usuario (lado del cliente) que comienza con el aseguramiento del navegador Web; en segundo lugar, asegurar el servidor y los datos que contiene (lado servidor) y por último asegurar la información que viaja entre el servidor Web y el usuario (canal de comunicación).

2.1.1 ASEGURAR LA COMPUTADORA DEL USUARIO

Se debe garantizar que la información y recursos de los usuarios estén seguros. Las fallas de seguridad en los navegadores, sumado a la falta de un antivirus, firewall [28] y otros mecanismos pueden permitir que los usuarios descarguen programas hostiles y expongan sus recursos. Para asegurar la computadora del usuario deben tenerse en cuenta las siguientes amenazas y los componentes existentes para mitigarlas.

2.1.1.1 Amenazas para el computador del usuario

La seguridad del computador de los usuarios se puede ver comprometida por el navegador Web que se esté utilizando para navegar y realizar transacciones B2C [29]. Esto puede suceder debido a la falta de actualización, configuraciones permisivas o por defectos presentes en los navegadores, falta de soporte antivirus, firewall, entre otros, las cuales facilitan a los atacantes comprometer las computadoras, información bancaria, transacciones y más.

Ahora, entre las principales amenazas que se pueden mencionar para el computador del usuario y primordialmente para el navegador Web, se tienen: las cookies[14] [30], los troyanos[15] [31] (keylogger), pharming [34], conexiones sin cifrar [32], configuraciones permisivas [32], defectos de los navegadores [32], software sin actualizar (antivirus, navegador, etc.), virus, contenido activo[16] [32] (Controles activeX, Java Scripts, Java Applets, plug-ins, VBScript).

Los troyanos o keylogger, en sus primeras versiones solo eran capaces de recolectar toda la información que se digitaba por el teclado, pero han evolucionado y en términos bancarios existen troyanos que solo se activan cuando el usuario esta en la pantalla de autenticación de la entidad financiera o las entidades que tiene como objetivo. Como mecanismo para evitar el escaneo de las teclas digitas por el usuario las aplicaciones bancarias o de pagos por Internet implementaron teclados virtuales, pero estos no son suficientes ya que existen Keyloggers que son capaces de grabar la porción de pantalla donde se están capturando los datos a través del teclado virtual para la transacción. Este tipo de Keyloggers utilizan, para la captura de video, dos librerías estándar: msvfw.dll y avifil32.dll encontradas por defecto en cualquier instalación de XP o Windows 2000 [31].

Por otro lado el protocolo de transferencia de hipertexto (HTTP) no permite el mantenimiento de la información después de múltiples peticiones y respuestas, y el comercio electrónico requiere de este mecanismo para garantizar su éxito. Las cookies fueron introducidas por Nestcape como mecanismo para solucionar este inconveniente, pero las objeciones referentes a los usos dados a las cookies se centran en poder mantener la privacidad de los datos de los usuarios, ya que por medio de estas se puede recolectar y recobrar información de los hábitos de navegación de los usuarios, claves, etc. que pueden ser fácilmente recolectados por el sitio Web que las alojó y que hoy en día han ganado gran valor comercial [30].

Otro aspecto a tener en cuenta referente a las Cookies es su tamaño, pues estas son extremadamente pequeñas (255 caracteres y menos 4 kbites) pero pueden almacenar información muy sensible: información de las páginas visitadas del firmante de la cookies, nombres de usuarios e incluso contraseñas de tarjetas de crédito, que en manos de un Cracker[17] [33] le permiten realizar acciones fraudulentas.

[14] Mecanismo para transferir y mantener información de estado de peticiones y respuestas http.

[15] Virus que se encarga de recolectar toda la información que se digita a través del teclado.

[16] Lenguajes de Script que permiten brindar mayor funcionalidad y mejorar la presentación de aplicaciones y páginas web.

[17] Persona con amplios conocimientos en informática capaz de romper sistemas informáticos para acceder a información que utilizará después de forma fraudulenta.

El pharming[18] es otra amenaza que hace uso de los navegadores, esta técnica permite la suplantación de páginas Web, y a través de estas el robo de información importante. Esta técnica es la evolución del phishing[19] [34] ya que se pueden engañar varias o cientos de personas a la vez gracias a que se intervienen las comunicaciones entre el usuario y su proveedor de Internet para de esta forma redireccionar todo lo que este digite a través de la barra de direcciones de su navegador web hacia páginas que suplanta las originales, principalmente se suplantan páginas de entidades financieras o de comercio.

El contenido activo, por otra parte, permite mayor funcionalidad y una mejor apariencia de las aplicaciones Web o sitios Web, todo esto se logra a través de la ejecución de programas por medio de scripts que utiliza el navegador Web, gracias a ellos se pueden mostrar diferentes tipos de menús y otras ayudas gráficas; desafortunadamente, los scripts son utilizados por los atacantes para descargar y ejecutar código malicioso. El contenido activo no siempre es peligroso, pero es la forma más popular que utilizan los atacantes para comprometer una computadora, y esto lo pueden hacer gracias a algunos problemas asociados a ellos: por ejemplo, el problema de los java applets radica en algunas vulnerabilidades de la maquina virtual de java [32], ya que estas vulnerabilidades permiten que los java applets se salten las restricciones del sandbox [32] donde la interacción con el resto del sistema debe ser limitada. Los plug-ins son similares a los Controles ActiveX, con la única diferencia de que estos no pueden ejecutarse fuera del navegador Web, pero con ellos se pueden lanzar ataques del tipo Buffer-overflows [29] o violaciones Cross-Domain [29]. En general el contenido activo se ve amenazado por múltiples vulnerabilidades como: cross-site scripting, Cross-Zone and Cross-Domain y detection evasión [29].

Como última amenaza que actúa en el navegador se tiene que mencionar el tipo de conexión. Si esta es cifrada o no, y si su nivel es alto, medio o bajo. El protocolo https es la versión segura de http. Https utiliza un cifrado seguro basado en SSL[20] para crear canales de comunicación seguros entre navegadores Web cliente y las páginas Web visitadas. Hay que recalcar que SSL solo garantiza la confidencialidad e integridad de los datos sobre la red, no garantiza la confidencialidad de la información en las páginas Web a las cuales viaja esta información.

A nivel general, los virus [35] son la principal amenaza en el computador del usuario (el cual se ve comprometido a través de los distintos tipos de navegadores Web) ya que gracias a ellos se puede robar información, realizar Pharming y todos los actos fraudulentos que comprometen la seguridad de los usuarios.

[18] Ataque que se realiza en el DNS (Domain Name System) que permite re direccionar una página Web suplantando su identidad.

[19] Técnica utilizada para recolectar información de forma fraudulenta a través de ingeniería social, su forma mas usual es la de suplantar personas o empresas mediante el uso de email.

[20] Para mayor entendimiento del protocolo SSL, ver la sección 1.1.3.1.2 de esta monografía.

2.1.1.2 Componentes necesarios para mitigar las amenazas presentes en el computador de los usuarios

- Anti-keyloggers.
- Navegadores Web que permitan gestionar las cookies y manejo de filtros anti-phishing.
- Antivirus para resguardar y monitorizar el computador del usuario.
- Certificados para garantizar la autenticidad de los sitios visitados.
- Certificados para garantizar la procedencia del contenido activo.
- Cortafuegos [36], para interponer entre la red y el equipo a proteger.
- Actualizaciones que permiten resolver las vulnerabilidades de los navegadores, sistemas operativos y software en general.

2.1.2 ASEGURAR LA INFORMACIÓN QUE VIAJA ENTRE EL SERVIDOR WEB Y EL USUARIO

Se debe garantizar que esta información no pueda ser leída, modificada ni destruida por terceros. Asegurar físicamente la red de forma que nunca se intercepten los datos sería utópico debido a su costo. Por eso la solución debe ser diferente, como por ejemplo, ocultar la información que se desea asegurar dentro de la información que parece no tener importancia. Esto es cifrar la información de forma que no pueda ser decodificada por nadie que no posea la llave correcta.

2.1.2.1 Riesgos para la información que viaja entre el Servidor Web y el usuario

Una conexión sin cifrado o con un nivel de cifrado inapropiado es la principal amenaza para la información que viaja entre el servidor Web y el usuario, ya que toda la información que viaja a través de la red se expone a escuchas ilegales hechas por medio de la utilización de Snnifers y a la perdida de la autenticidad de la misma al ser interceptada y modificada [28].

2.1.2.2 Componentes necesarios para mitigar las amenazas de la información que viaja entre el servidor Web y el usuario

- Protocolos. (Para mayor información ver sección 1.1.3.1).
- Sistemas criptográficos para cifrar la información. (Para mayor información ver sección 1.1.3.4).

2.1.3 ASEGURAR EL SERVIDOR Y LOS DATOS QUE CONTIENE

La información que reside en el servidor debe ser modificada sólo por quienes poseen la autorización para ello; debe ser distribuida sólo a quienes se debe distribuir.

2.1.3.1 Riesgos Presentes en los servidores

Hablar de un servidor Web seguro no sólo significa que este utilicé una conexión segura hacia y desde los navegadores Web, también existen otra serie de requerimientos y riesgos que deben cubrirse para garantizar la seguridad y confidencialidad de los datos, del mismo sitio o de sus usuarios, que en el se puedan almacenar.
Estos riesgos y requerimientos pueden cubrirse o entenderse partiendo de la definición de lo que es un servidor Web seguro: Es un programa que incorpora sistemas criptográficos para garantizar la confidencialidad de la información que viaja a través de la red, además de ser el encargado de resguardar la información de los usuarios y del mismo sitio, permitiendo que la información que en él resida solo sea accesada y procesada por quienes posean los suficientes privilegios de seguridad para tal fin [28]. En conclusión los principales riesgos son la forma en que es enviada la información desde los servidores Web hacia los clientes y cómo la información que llega desde estos es mantenida para garantizar su confidencialidad y autenticidad.

Otro aspecto clave y que incorpora en algunas ocasiones factores de riesgo tiene que ver con las políticas de privacidad [37] del sitio Web, porque aunque el sitio garantice la seguridad de los datos que aloja en sus servidores, algunas políticas permiten el manejo o traspasan la información a terceras partes. Además, existen servidores que se quedan con información que sólo corresponde a los bancos, esto sucede cuando los servidores que alojan los sitios Web no utilizan pasarelas de pago o protocolos como SET que fueron desarrollados para tal fin.

2.1.3.2 Componentes necesarios para asegurar el servidor y los datos que contiene.

- Conexiones seguras.
- Políticas de privacidad de la información.
- Sistemas criptográficos.
- Firewall.

2.2 RECOMENDACIONES Y POLÍTICAS DE SEGURIDAD EXISTENTES EN TRANSACCIONES DE COMECIO ELECTRÓNICO B2C

En este capítulo se recopilaron las principales políticas existentes para la realización de transacciones de comercio electrónico tipo B2C. Se exploraron las páginas Web de los principales bancos nacionales, de entidades emisoras de tarjetas crédito y/o débito y

algunas casas desarrolladoras de antivirus. Cabe recalcar que no se encuentran políticas desarrolladas para la realización de transacciones con tarjetas crédito ó débito orientadas hacia los usuarios; las políticas que se encuentran aquí, son políticas de seguridad implementadas por las entidades para resguardar su propia seguridad y políticas de privacidad que le indican a los usuarios cual será el manejo que se hará de su información. A continuación se exponen las principales recomendaciones y políticas de seguridad y privacidad desarrolladas por ellos.

Para abordar las distintas políticas y recomendaciones se hace necesario distinguir, como primera medida, las diferencias entre lo que es una política y una recomendación; lo mismo que diferenciar entre una política de seguridad y una política de privacidad.

- **Definición de Política de Seguridad**

Una política de seguridad declara un conjunto de lineamientos obligatorios que deben seguirse dentro de una organización para garantizar la seguridad de los activos más importantes para esta. La efectividad de las políticas de seguridad radica en su diseño, implementación y mantenimiento, pues una política implementada sin tener en consideración estas etapas corre el peligro de no ser tenida en cuenta, de parecer incompleta o de ser redundante.

Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por mejores prácticas, procedimientos y recomendaciones. Las políticas deben ser pocas y deben ofrecer direccionamientos a toda la organización [8].

Según RFC 2196 [7], que es una guía para desarrollar políticas de seguridad y procedimientos para los sitios que disponen de sistemas a través de Internet, estas son las características que debe cumplir una buena política de seguridad:

- Deben existir mecanismos o procedimientos concretos que permitan su implementación o puesta en práctica, estos mecanismos deben ser los más apropiados y prácticos.

- Se deben utilizar herramientas de seguridad para obligar su cumplimiento.

- Deben poseer mecanismos de control para valorar la efectividad de las herramientas de seguridad utilizadas.

- **Definición de Mejor Práctica**

Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de

manera uniforme, garantizando un nivel consistente de seguridad a través de la organización [8][8].

- **Definición de Recomendación**

Una recomendación es una declaración general utilizada para sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las recomendaciones deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo [8].

- **Definición de Procedimiento**

Los procedimientos definen específicamente cómo las políticas, mejores prácticas y recomendaciones serán implementadas en una situación dada. Los procedimientos son dependientes de la tecnología y se refieren a plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos para implementar la seguridad relacionada a dicho sistema específico [8].

- **Definición de Política de Privacidad**

Una política de privacidad expone el trato que se le dará a los datos brindados por usuarios.

2.2.1 Políticas y recomendaciones expuestas por bancos nacionales (Sucursales Virtuales)

Los Bancos Nacionales, presentan la facilidad a sus usuarios de realizar transacciones bancarias por medio de Sucursales Virtuales, en las cuales se catalogan algunas políticas implementadas para garantizar la seguridad en las transacciones y recomendaciones hechas a los usuarios para hacer más seguras las mismas:

2.2.1.1 Políticas de Privacidad implementadas por Bancos

Entre las políticas de privacidad implementadas por las entidades bancarias para garantizar la privacidad de los datos de los usuarios tenemos:

- Utilizar claves personales sólo cuando la privacidad no está siendo violada.
- Siempre se deben terminar las operaciones o cerrar la sesión antes de retirarse de cualquier medio donde se requiera digitar la clave personal.
- Al actualizar datos a través de la sucursal virtual se debe verificar la autenticidad de la misma por medio de sus certificados digitales.

- El Banco nunca solicita información confidencial para la actualización de datos relacionados con los números de la tarjeta débito o crédito y claves correspondientes.

- Varios navegadores o browsers permiten almacenar las contraseñas que se le solicitan en algunos sitios. Debido a que otras personas pueden tener acceso a esa información, no es recomendable hacer uso de esta opción.

2.2.1.2 Políticas de Seguridad implementadas por los Bancos

Algunas de las políticas de seguridad implementadas para garantizar la seguridad a nivel bancario son las siguientes:

- Certificación de las páginas Web con entidades emisoras de certificados, tal como Verising.

- Encriptación de datos.

- Utilización de conexiones seguras.

- Control de acceso al servidor Web.

- Identificación de usuarios.

- Utilización de antivirus y software de prevención Anti-Spyware y Anti-phishing.

2.2.1.3 Recomendaciones Bancos

- Actualizar el antivirus.

- Instalar un firewall, este avisará de la entrada de datos sin permiso y de salida de información sin autorización.

- Evitar el envió de correo masivo.

- Verificar siempre que tu navegador haya establecido una conexión segura cuando se hagan compras o envíe información importante a través de Internet.

- Ingresar a las sucursales virtuales directamente desde la barra de direcciones de tu navegador.

- Verificar las direcciones que se digitan, ya que los errores en estas están siendo utilizados para realizar phishing.
- Cambiar frecuentemente las claves digitales.
- No utilizar computadores públicos.

2.2.2 Políticas Emisores de tarjetas crédito y debito

Entre los principales emisores de tarjetas de crédito y débito a nivel nacional e internacional tenemos a VISA, American Express, Dinners Club, Master Card y el Banco de Occidente. A continuación se exponen un conjunto de políticas y recomendaciones propuestas por ellos para realización de transacciones con tarjetas de crédito y debito.

2.2.2.1 Políticas de seguridad.

- Aseguramiento de sesiones y conexiones seguras.

2.2.2.2 Políticas de privacidad

- Establecimiento de sesiones y conexiones seguras.

2.2.2.3 Recomendaciones

- No aceptar correos electrónicos que pidan darse de baja de algún servicio o actualización de cuentas.
- Evitar enviar por correo información financiera.
- Usar un explorador seguro.
- Actualizar y utilizar las últimas versiones de exploradores.
- Identificar con quien se hace transacciones.
- Mantener las contraseñas secretas.
- Guardar una copia de las transacciones.
- Utilizar contraseñas adicionales, ejemplo Verified for Visa [38], que brindan mayor seguridad en las transacciones.
- Digitar directamente la dirección de las entidades bancarias y de comercio directamente en la barra de direcciones de su explorador.

- Verificar que su explorador ha establecido una conexión segura.

- Verificar que el sitio en el cual realiza sus compras es seguro.

Los bancos y entidades emisoras de tarjetas de crédito y débito no presentan políticas de seguridad a sus clientes; estas organizaciones solamente exponen un conjunto de recomendaciones y mejores prácticas para la realización de transacciones electrónicas. Erróneamente a estas recomendaciones las denominan políticas de seguridad, ya que solamente las dejan enunciadas en sus portales Web, pero no las implementan. Dichas organizaciones dejan la responsabilidad al usuario sobre el manejo de sus datos, ya que no tienen en cuenta el conocimiento que el usuario pueda tener sobre la seguridad en la transacción en si y los aspectos relevantes a tener en cuenta en el mismo equipo.

2.2.3 Recomendaciones inteligentes Norton (Symantec)

Norton de Symantec la seguridad de las transacciones comerciales en línea comienza con estos hábitos [25]:

- Realizar conexiones y transacciones en sitios encriptados ya que las páginas encriptadas cifran las contraseñas, nombres de usuario y números de tarjetas de crédito antes de enviarlos.

- Verificar la autenticidad de los sitios - En un sitio autenticado puede tener la certeza de que no está accediendo a una página falsa.

- Utilizar tarjetas de crédito para las compras en Internet.

- Adoptar nombres de usuario y contraseñas difíciles de averiguar, y cambiarlos con frecuencia.

- Proteger su identidad - No revelar nunca el número de un documento identificativo u otra información personal por Internet.

3 FORMULACIÓN DE LAS POLÍTICAS Y RECOMENDACIONES DE SEGURIDAD NECESARIAS PARA MINIMIZAR LOS RIESGOS EN TRANSACCIONES DE COMERCIO ELECTRÓNICO B2C

La formulación de políticas no es algo que se realice al azar, existen una serie de estándares y guías utilizadas para la creación y gestión de las mismas, entre las más significativas tenemos: RFC 2196 [7] y la ISO 17799 [6]**¡Error! No se encuentra el origen de la referencia.**. El RFC 2196 es una guía para la creación de políticas de sitios que se encuentran en Internet, mientras que la ISO 17799 es un código de prácticas de Seguridad en Gestión de la Información [40], pero a pesar de ser tan específicos son una estupenda guía para la creación, diseño y mantenimiento de políticas de seguridad que constituyen parte del ciclo de vida de cualquier política y han sido tomados como punto base, en este y otros trabajos, para la realización de modelos que permitan crear y mantener políticas de seguridad.

3.1 ETAPAS DEL CICLO DE VIDA DE LAS POLÍTICAS DE SEGURIDAD

Según la metodología adoptada por la Universidad Nacional de Colombia en su guía para la Elaboración de Políticas de Seguridad, la cual es un texto traducido y adaptado del libro "The Security Policy Life Cicle: Functions and Responsabilities" [8][8], las siguientes etapas permiten el diseño, implementación y mantenimiento de cualquier tipo de política de seguridad. En la Figura 3.1 se observa el ciclo de vida de una política de seguridad. (Ver Anexo B).

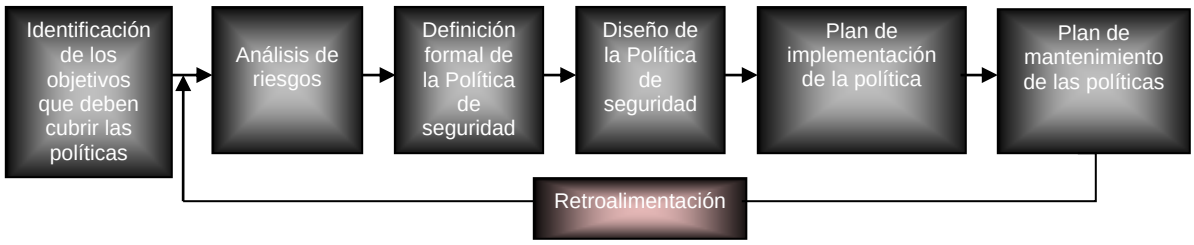

Figura 3.1 Ciclo de vida de una política de seguridad para transacciones B2C

3.1.1 IDENTIFICACIÓN DE LOS OBJETIVOS QUE DEBEN CUBRIR LAS POLÍTICAS

Como primera medida la creación de políticas requiere que se identifiquen los objetivos que deben cubrir las políticas además de su alcance, la Tabla 3.1 muestra esto en detalle.

OBJETIVOS	ALCANCE
Garantizar la autenticidad de los sitios de comercio electrónico	Se debe garantizar la autenticidad de los sitios de comercio electrónico para evitar problemas de tipo phishing.
Garantizar la privacidad o confidencialidad de la información	La información solo debe ser accedida por las personas o sistemas con los permisos necesarios para tal fin.
Garantizar el no repudio de las transacciones	Lado cliente y sitios de comercio electrónico.
Garantizar la integridad de los datos	Garantizar la integridad de los datos que viajan a través de la red.
Garantizar un nivel de seguridad mínimo para la realización de las transacciones	Solo del lado cliente.

Tabla 3.1 objetivos y alcance de las políticas

3.1.2 ANÁLISIS DE RIESGOS

El análisis de riesgos es de interés para aquellas personas que trabajan con información y con los sistemas que los sustentan, ya que gracias a este análisis se puede hallar el valor de los activos, la cantidad que puede estar en juego y la forma de protegerlos. El primer paso en la realización del análisis de riesgos debe ser la estructuración del proyecto de análisis de riesgo (ver Figura 3.2) el cual presenta las etapas necesarias para la consecución del mismo.

3.1.2.1 Estructuración del proyecto de análisis de riesgo.

Son los pasos necesarios para concebir el proceso de análisis y gestión del riesgo, se debe escoger una estructura cíclica ya que los sistemas de información son elementos que no se mantienen inmutables.

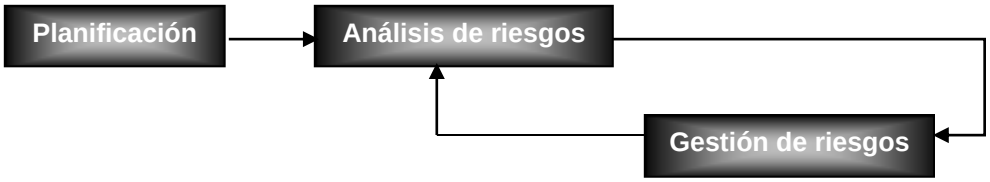

Figura 3.2 Estructura del proyecto de análisis de riesgos

- **PLANIFICACIÓN**

En cuanto a la planificación se ha tomado como decisión identificar sólo los objetivos y el alcance del proceso de análisis de riesgo, en este punto la metodología tiene en cuenta más pasos que se pueden tomar de acuerdo al tipo de organización.

Objetivos:

- Identificar las principales amenazas que afectan las transacciones hechas con tarjetas de crédito o débito en entornos de comercio electrónico B2C.

- Identificar los requerimientos principales de seguridad para garantizar la autenticidad de las partes, privacidad o confidencialidad de la información, el no repudio de las transacciones y la integridad de los datos en tránsito.

- Identificar el nivel de los riesgos asociados a los diferentes activos involucrados en transacciones B2C, con tarjeta crédito y débito.

- Hallar los mecanismos o controles necesarios para mitigar los riesgos encontrados.

Alcance del proceso de análisis de riesgos

El análisis de riesgo se realizará para aquellas amenazas presentes en transacciones B2C realizadas con tarjetas crédito y/o débito, a través de computadores de escritorio, y para aquellos riesgos que tienen incidencia en el lado cliente. Como referente se toman los datos encontrados en el Capítulo 2 de esta monografía que constituyen gran parte de los elementos involucrados en transacciones B2C y las amenazas a las que estos se enfrentan.

▪ ANÁLISIS DE RIESGOS

El análisis de riesgos es útil para determinar los activos que le dan valor a la organización. Los elementos incluidos dentro del análisis de riesgos son: los activos, amenazas y salvaguardas. Con estos elementos se puede calcular el impacto (lo que podría pasar) y el riesgo (lo que posiblemente pase).
La aproximación metódica implica seguir los siguientes pasos:

1. Determinar los activos importantes, sus dependencias y valores, en el sentido de qué perjuicio (coste) supondría su degradación (Modelo de valor).

2. Determinación de las amenazas y vulnerabilidades a las cuales están expuestos los activos (Mapa de riesgos).

3. Determinación de las salvaguardas existentes y de la eficacia de las mismas, inicialmente este punto no se realiza ya que no existen salvaguardas aplicadas.

4. Estimar el riesgo, definido como el impacto ponderado por la tasa de ocurrencia (o expectativa de materialización) de la amenaza. Esto incluye estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

1. Modelo de valor

- **Definición de activos**

  Los activos son los elementos del sistema de información o elementos relacionados con este los cuales brindan valor a la organización; en el caso particular de este proyecto son aquellos elementos que intervienen en una transacción B2C.

  En el Anexo C, Tabla 3.3, se listan los principales activos, su descripción y el tipo al que pertenece cada activo. Esta clasificación por tipos se puede encontrar en el Catálogo de Elementos de la metodología Magerit [41].
  En ella se encuentran nueve tipos de clasificación ordenados según su importancia: datos, servicios, aplicaciones, equipos informáticos, redes de comunicaciones, soporte de información, equipamiento auxiliar, instalaciones, y personal. En el caso particular de este proyecto los activos están clasificados en servicios, datos y aplicaciones.

- **Dependencias entre activos**

  Es común encontrar que los activos más significativos para la organización dependan de otros activos menos significativos, esta dependencia hace que su valoración cambie o se vea impactada de otra manera por lo cual se hace importante encontrar las dependencias entre todos los activos (ver Anexo C Tabla 3.4). Gracias a las dependencias entre activos se puede obtener un árbol de las mismas que permite tener una visión mas clara de las dependencias obtenidas.

  En la figura 3.2 del Anexo C se han distribuido los activos en dos capas (superior e inferior) esta distribución se realiza con el fin de ofrecer una mejor vista de la dependencia existente entre los activos, y lo que nos dice, es que existe una capa superior que no ofrece dependencias hacia otras capas y en la cual se encuentran activos que depende de otros ubicados en una capa inferior los cuales los afectan directamente.

- **Estructuración de los activos**

  Los activos clasificados anteriormente se estructuran en tres tipos de capas. Esto se realiza en base a los criterios establecidos en la metodología de Magerit [41], en el cual el libro de Catálogos especifica la clasificación en la que se encuentra cada activo. (Ver Tabla 3.2).

ACTIVOS					
Capa Superior Datos / Información		**Capa Intermedia Servicios**		**Capa Inferior Aplicaciones Software**	
[s]	Información de acceso y financiera (Número cuenta, clave tarjeta, contraseñas, etc.)	**[pki]**	Sistemas criptográficos. Certificados Digitales.	**[browser]**	Navegador.
[com]	Certificados digitales.			**[av]**	Antivirus.
				[fw]	Cortafuegos.
				[com]	Certificados digitales.

Tabla 3.2 Estructuración de activos por capas

En la tabla 7 se puede ver una clasificación de los activos según su importancia, esta nos dice que en una capa superior se encuentran los datos los cuales son soportados por las capas intermedia (servicios) y por la capa inferior (aplicaciones) las cuales deben brindar soporte al tratamiento de los datos y seguridad de los mismos.

- **Valoración global de los activos por su uso**

  En la tabla 3.6 del Anexo C se obtienen datos estadísticos sobre el uso de ciertos activos que son necesarios para la realización de transacciones electrónicas.
  Los resultados del uso de los activos como Información de acceso y financiera, Antivirus, Sistemas Criptográficos y Firewall son obtenidos de la fuente de INTECO [42]. Mientras que el porcentaje de uso del navegador (%100) se da debido a que este elemento es imprescindible a la hora de realizar una transacción B2C o simplemente navegar por internet:

- **Dimensiones de valoración de los activos**

  Son las características o atributos que hacen valioso un activo (Ver Anexo C Tabla 3.2). Una dimensión es una faceta o aspecto de un activo independiente de otras facetas. Puede realizarse análisis de riesgos centrado en una única faceta, independiente de lo que ocurra con otros aspectos.

  Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza [41]. La valorización que recibe un activo en cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

En la tabla 3.2 del Anexo C se han valorado los activos de acuerdo a las dimensiones de valoración que afectan, signo @ para aquellas dimensiones afectadas por cada activo, este valor se obtuvo de forma cualitativa y expresa la importancia del activo a través de las dimensiones.

Con los datos obtenidos hasta aquí y junto con el cálculo del impacto, frecuencia de ocurrencias y demás datos necesarios se podrá obtener la medida del riesgo final.

2. Mapa de Riesgos, Amenazas y Vulnerabilidades por Activos

El mapa de riesgos es el resultado de la siguiente relación:
Activo – Amenaza – Vulnerabilidades. Esta relación se puede observar en la Tabla 3.7 del Anexo C.

3. Estimación del Riesgo

Una vez se determina que una amenaza puede afectar un activo hay que estimar el nivel de vulnerabilidad del activo; para esto se calculan valores en dos sentidos:

Primero

La Frecuencia: Esto es cada cuanto se va a materializar la amenaza.

La Degradación: Cuanto se perjudica el activo con la materialización de la amenaza.

Segundo

Impacto = Valor * Degradación.

Riesgo = Impacto * Frecuencia.

Con la obtención de esta formulación se tiene estimado el riesgo del sistema, activo por activo.

- **Calculo del impacto económico**:

Realizar un análisis por tabla permite realizar un análisis cuantitativo del impacto económico y aunque esta misma aproximación pudo haberse tomado para calcular la probabilidad de ocurrencia, se optó por realizar un análisis cuantitativo gracias a algunos valores brindados por INTECO [43], [44], [45]. La Figura 3.1 del Anexo C muestra los criterios tomados para valorar el impacto económico y la degradación de los activos, mientras que la Tabla 3.8 del Anexo C muestra el impacto económico por activo.

- **Cálculo del riesgo**

Para hallar el valor de la Medición del Riesgo, se debe multiplicar el impacto por la probabilidad de ocurrencia:

Activos	Amenazas	Vulnerabilidades	Impacto económico	Probabilidad de ocurrencia	Medición del Riesgo
Antivirus	Nuevos virus	Necesidad de actualizaciones y parches de seguridad.	70	0.359	25.13
	Ataques del día cero	Tipo de Protección Reactiva.	70	0.690	48.3
Navegador Web	Virus en general	Configuración por defecto.	56	0.086	4.816
	Cookies	Configuración por defecto.	8	1	8
	Keyloggers + Troyanos	Teclados virtuales + ausencia de soporte antikeyloggers + teclados físicos + falta de soporte antivirus.	80	0.527	42.16
	Phishing, pharming y similares.	Navegadores sin soporte antiphishing.	80	0.299	23.92
	Conexiones a sitios sin utilizar cifrado o cifrado deficiente.	Autonomía del navegador para permitir conexiones sin cifrar.	80	0.734	58.72
	Código activo.	Configuración del navegador para aceptar controles activeX, plug-ins, java script, Visual Basic script, java applets.	24	0.3	7.2
Firewall	Virus en general	Configuración por defecto o configuraciones muy permisivas.	70	0.086	6.02
Certificados Digitales	Suplantación de identidad.	Falta de verificación por parte de los usuarios la autenticidad del sitio.	10	0.760	7.60
Sistemas criptográficos	Ataques para descifrar la información	Longitud corta de las claves utilizadas para generar contraseñas y algoritmos de cifrado deficientes.	12	0.5	6
Información	Virus en general	Almacenamiento sin	20	0.086	1.72

de acceso y financiera (Claves y contraseñas)		cifrar.			
	Obtención fraudulenta	Falta de soporte antiphishing.	20	0.146	2.92
	Keyloggers + Troyanos	Falta de soporte antikeyloggers y antivirus.	20	0.527	10.54

Tabla 3.3 Calculo del riesgo

- **Interpretación de los resultados**

  En la interpretación de los resultados se busca establecer relaciones de prioridad por activos o grupos de activos, ya sea por orden de impacto o por orden de riesgo. En este caso particular, se utilizó el Criterio de Medición del Riesgo por Activos, teniendo en cuenta las dependencias entre cada uno de ellos, para obtener el valor acumulado del riesgo (Ver Anexo C):

Activo: Certificados Digitales		
Amenazas	**Priorización**	**Valor acumulado**
Suplantación de identidad.	1	7.6
Activo: Navegador Web		
Amenazas	**Priorización**	**Valor acumulado**
Conexiones a sitios sin utilizar cifrado o cifrado deficiente.	1	58.72
Keyloggers + troyanos	2	42.16
Phishing, pharming y similares	3	23.92
Cookies	4	8
Activo: Información de acceso y financiera (Claves y contraseñas)		
Amenazas	**Priorización**	**Valor acumulado**
Keyloggers + troyanos	1	10.54
Obtención fraudulenta	2	2.92
Virus en general	3	1.72
Activo: Sistemas Criptográficos		
Amenazas	**Priorización**	**Valor acumulado**
Ataques para descifrar la información	1	6
Activo: Antivirus		
Amenazas	**Priorización**	**Valor acumulado**
Ataques del día cero	1	48.3
Nuevos virus	2	25.13
Activo: Firewall		
Amenazas	**Priorización**	**Valor acumulado**
Virus en general	1	6.02

Tabla 3.4 Priorización de las amenazas por activos

La tabla anterior presenta el valor acumulado del riesgo, el cual se ha priorizado teniendo en cuenta las dependencias entre los activos.

- **GESTIÓN DEL RIESGO**

Al combinarse impacto y probabilidad de ocurrencia se obtiene el nivel de riesgo. Para aquellos niveles cuyo valor sea muy alto se debe planificar inmediatamente el tipo de salvaguardas necesarias para mitigar la fuente de riesgo o transferirla.

Eliminar la fuente de riesgo es imposible por esto el método a seguir es tratar de mitigarlos actuando preventivamente para que no ocurra. El método utilizado para esto será la implementación de políticas y recomendaciones. Para lograr un seguimiento de la política, esta debe poseer un diseño con elementos para tal fin; dichos elementos se detallan en el siguiente capítulo.

3.1.3 DEFINICIÓN Y DISEÑO DE LA POLÍTICA DE SEGURIDAD

En la Tabla 3.4 se priorizan cada una de las amenazas, de acuerdo a los lineamientos establecidos en Magerit versión 2. La priorización de cada una de ellas se realiza en base al valor del riesgo asociado; para el caso de los activos, que tengan dependencias, en los que estas amenazas actúan se tiene en cuenta el valor acumulado asociado.

De esta manera, como mecanismo para la reducción del riesgo se ha seleccionado el uso de políticas de seguridad, las cuales se van a implementar para aquellos activos cuyo valor acumulado sea mayor; mientras que para los activos cuyo valor sea más bajo, se decide aceptar el riesgo y brindar una recomendación.
De igual forma existen prácticas que son difíciles de controlar, o de hacer obligatorias para que los usuarios las cumplan, o tienen un costo relativamente alto o de difícil implementación; por lo cual, el uso de recomendaciones aparece nuevamente como mecanismo para actuar contra el riesgo. En la siguiente tabla (Tabla 3.5) se ilustran las estrategias seleccionadas para mitigar o controlar cada riesgo:

Activos	Amenazas	Salvaguarda
Antivirus	Nuevos virus	Recomendación.
	Ataques del día cero	Recomendación.
Navegador Web	Virus en general	Recomendación.
	Cookies	Recomendación.
	Keyloggers + Troyanos	Política.
	Phishing, pharming y similares	Recomendación.

	Conexiones a sitios sin utilizar cifrado o cifrado deficiente Alojamiento de Scripts	Política. Recomendación.
Firewall	Virus en general	Recomendación.
Certificados Digitales	Suplantación	Política.
Sistemas Criptográficos	Ataques para descifrar la información	Recomendación.
Información de acceso y financiera (Claves y contraseñas)	Virus en general Obtención fraudulenta Keyloggers + Troyanos	Recomendación. Recomendación. Política.

Tabla 3.5 Estrategias para mitigar los niveles de riesgo

A continuación se muestran las políticas seleccionadas que trataran de mitigar el riesgo asociado a cada una de las amenazas. Estas políticas siguen el diseño establecido para la definición de las mismas (Ver Anexo B figura 2.2):

POLITICA: Se debe verificar la identidad del sitio de comercio electrónico en el cual se realizan compras.	
Responsable: **Freddy Mina G.**	
RELACION AMENAZA Suplantación de Identidad	***DESCRIPCION*** Esta política debe permitir la identificación del sitio de comercio electrónico para evitar ataques de tipo phishing.
Excepciones: **ninguna**	
Fecha de creación: 20 de julio de 2008 ***Fechas últimas revisiones:*** 10 de agosto de 2008, 2 de enero de 2009. ***Estado de la Política:*** *En uso* ***Identificador:*** 001-IdentiSyte	
Anotaciones Verificación de las partes esenciales dentro de un certificado digital 2 de enero de 2009. Próxima revisión pendiente julio de 2009.	
Estándares u orientaciones	• Utilizar navegadores actualizados que permitan esta verificación. • Utilizar navegadores con soporte de certificados extended validation para realizar una verificación inicial de forma visual.
Mejor Practica	• Nunca llegar a los sitios Web a través de vínculos de terceros, digitar directamente la dirección en la barra

	de direcciones del navegador. • Verificar la autenticidad del sitio Web a través de la información de la página.
Guías	❖ La verificación de la utilización de la tecnología Extended Validation en exploradores como internet Explorer 7 o Mozilla Firefox 3.0.8 se hace de forma visual, la barra de direcciones en ambos navegadores se torna de color verde cuando un sitio utiliza un certificado de este tipo. ❖ La información de la página, en el explorador Mozilla, se puede acceder a través de la barra de herramientas, en el link herramienta, información de la página (tipo de certificado, quien los firmo, issuer, etc).
Dimensiones que afecta	• Autenticidad. • Integridad.
Consecuencias del no cumplimiento	• Robo de información financiera. • Realización de transacciones fraudulentas.

Tabla 3.6 Política identificación del sitio de comercio B2C

POLITICA: Verificar que durante la transacción se haya establecido una conexión segura entre el navegador web y el sitio de comercio electrónico.	
Responsable: **Erwin Daza Rendón**	
RELACION AMENAZA Conexiones a sitios sin utilizar cifrado o cifrado deficiente	***DESCRIPCION*** Esta política debe permitir que se utilice el cifrado, con un nivel de seguridad aceptable, de la información que viaja entre el navegador y el sitio de comercio.
Excepciones: **ninguna**	
Fecha de creación: 20 de julio de 2008 ***Fechas últimas revisiones:*** 10 de agosto de 2008, 5 de enero de 2009 ***Estado De la Política:*** *En uso* ***Identificador:*** 001-ConexToSyte	
Anotaciones Verificación del tipo de protocolo utilizado para la conexión entre el navegador y el servidor que aloja la el sitio Web, 5 de enero de 2009.	
Estándares u orientaciones	• Utilizar el protocolo SSL 3.0, TLS1 o SET que garantiza cifrado de datos y conexiones seguras. • Verificar en la información de la página el tipo de conexión y el nivel de cifrado.
Mejor Practica	✓ En el navegador Mozilla Firefox 3.0.8, la selección del protocolo para el cifrado, se configura desde la opción: herramientas – opciones – avanzado –

	cifrado. Se puede seleccionar tanto el protocolo SSL 3.0 como el TLS1. En la parte de selección de certificados para sitios web que no posean uno, seleccionar "preguntar cada vez". ✓ Configurar las advertencias de seguridad desde: herramientas, opciones, seguridad, mensajes de advertencia, configuración.
Guías	❖ Para ver la información del tipo de cifrado y su nivel, se accede en Mozilla a través de la barra de herramientas, en el link herramientas, información de la página. ❖ De forma visual se puede hacer verificando que en la barra de direcciones se utilicé HTTPS en lugar de HTTP.
Dimensiones que afecta	• Privacidad o confidencialidad. • Integridad. • Autenticidad.
Consecuencias del no cumplimiento	• Robo de información. • Perdida de integridad de los datos enviados y recibidos. • Realización de transacciones con sitios de dudosa reputación

Tabla 3.7 Política verificación de la conexión

POLITICA: Verificar el soporte antivirus y firewall.	
Responsable: **Freddy Mina**	
RELACION AMENAZA Virus en general	***DESCRIPCION*** Esta política permite verificar que el software antivirus este instalado al igual que el firewall el cual debe estar activado.
Excepciones: **ninguna**	
Fecha de creación: 25 de julio de 2008 ***Fechas últimas revisiones:*** 10 de agosto de 2008, 8 de enero de 2009 ***Estado de la Política:*** *En uso* ***Identificador:*** 001-suportAntiV-FirEnable	
Anotaciones Verificación del antivirus instalado en la máquina local del usuario y verificación del estado del firewall del sistema operativo, 8 de enero de 2009.	
Estándares u orientaciones	Utilizar Firewall de IPTABLES, estos están integrados en el kernel, son parte del sistema operativo y se pone en marcha aplicando reglas.
Mejor Practica	• Configurar el firewall con una política por defecto de denegar todo, solo aceptar aquello que este explícitamente especificado por las reglas.

	• Bloquear aquellos puertos que no son fundamentales, en especial el puerto 23 (Telnet). • Verificar puertos abiertos y crear reglas para protegerlos. • Crear un registro de seguridad el cual almacena intentos fallidos y exitosos de conexiones; útil a la hora de resolver problemas.
Guías	
Dimensiones que afecta	• Privacidad o confidencialidad, integridad y autenticidad
Consecuencias del no cumplimiento	• Robo de información. • Perdida o daño del sistema operativo. • Afectación de los recursos del sistema.

Tabla 3.8 Política para la verificación del soporte del equipo

POLITICA: Verificar la actualización del navegador.	
Responsable: **Erwin Daza Rendón**	
RELACION AMENAZA Virus en general, phishing, pharming y similares.	***DESCRIPCION*** Esta política permite verificar el nivel de actualización del navegador, gracias a esto se pueden obtener soporte antiphising y evitar vulnerabilidades.
Excepciones: **ninguna**	
Fecha de creación: 10 de agosto de 2008 ***Fechas últimas revisiones:*** 21 de agosto de 2008, 20 de enero de 2009. ***Estado De la Política:*** *En uso* ***Identificador:*** 001-ActualizacionNav	
Anotaciones Pendiente Verificación de nuevas vulnerabilidades en relación al motor de renderizado de Mozilla, ultima versión del gecko-sdk 1.9.0.0.1.	
Estándares u orientaciones	• Instalar las últimas versiones de los navegadores, recomendable aquellos con una versión del gecko igual o superior al 1.8.
Mejor Practica	Verificar lista de sitios dedicados al phishing.
Guías	
Dimensiones que afecta	• Privacidad o confidencialidad, integridad y autenticidad
Consecuencias del no cumplimiento	• Comprometimiento del navegador.

Tabla 3.9 Política para la verificación del nivel de actualización del navegador

Amenaza	***Recomendaciones***	***Dimensiones que afecta***	***Consecuencia del no cumplimiento***
Nuevo Virus	❖ Se debe mantener el Antivirus actualizado. ❖ Mantener el sistema operativo actualizado con todos los parches de seguridad.	• Confidencialidad. • Integridad. • Disponibilidad.	• Infección del sistema (computador) por causa de los nuevos virus. • Perdida de información. • Perdida del sistema operativo. • Infecciones a otros equipos
Ataques del Día Cero	❖ Están enterados de los últimos boletines acerca de nuevos virus. ❖ Actualizar el antivirus constantemente.	• Confidencialidad. • Integridad. • Disponibilidad.	• Infección del sistema (computador) por causa de los nuevos virus.
Virus en general	❖ Instalación de un software antivirus. ❖ Actualizar el antivirus constantemente	• Confidencialidad. • Integridad. • Disponibilidad	• Infección del sistema (computador) por causa de virus (nuevos y antiguos).
Cookies	❖ Verificar las políticas de privacidad de los sitios antes de permitirles utilizar cookies. ❖ Utilizar tecnologías como P3P que le permiten verificar sus preferencias de privacidad con las políticas de privacidad de los sitios. ❖ Configurar el navegador para no aceptar cookies. ❖ Si por alguna razón permite el uso de cookies configure su navegado para que las elimine	• Confidencialidad	• Distribución de su información a terceras partes. • Robo de información.

	al cerrarse este.		
Phishing pharming y similares	❖ Utilizar navegadores con soporte antiphishing. ❖ Utilizar antivirus con soporte antiphishing	• Confidencialidad	• Robo y suplantación de identidad
Alojamiento de Scripts	❖ Permitir solo Script de páginas reconocidas. ❖ Permitir solo Scripts que contengan certificados	• Confidencialidad. • Integridad.	• Perdida de información. • Infección del sistema.
Obtención fraudulenta de claves y contraseñas	❖ No envía sus datos por medio de conexiones sin cifrar. ❖ Instale un software antivirus y manténgalo actualizado.	• Confidencialidad.	• Realización de fraudes con las claves y contraseñas robadas.
Ataques para descifrar la información	❖ No envía sus datos por medio de conexiones sin cifrar.	• Confidencialidad. • Integridad.	• Robo de información. • Perdida de la integridad de la información enviada

Tabla 3.10 Comparación amenazas contra recomendación

Las políticas y recomendaciones mostradas aquí pretenden mitigar y controlar los riesgos encontrados inicialmente: es muy posible que estas políticas cambien en el tiempo dando cabida a nuevas políticas o a la adaptación de las ya existentes, esto debido a requerimientos de seguridad que surjan en el tiempo, de igual forma, puede darse que aquellas recomendaciones adoptadas aquí puedan migrar hacia la categoría de políticas dependiendo de la aparición de nuevos riesgos y de la gestión que se le deba dar al mismo.

4 PLAN DE DISEÑO E IMPLEMENTACIÓN DE POLÍTICAS Y RECOMENDACIONES DE SEGURIDAD

Las políticas desarrolladas en el capítulo anterior deben ser utilizadas por usuarios de transacciones B2C, pero debido a que estos desconocen en alguna medida los temas concernientes a la seguridad que deben implementar, y pese a que exista un conjunto de políticas y recomendaciones, siempre habrá un grado de dificultad a la hora de ponerlas en práctica; por esta razón, se ha decidió automatizar el conjunto de políticas y dejar libre al usuario de ejecutarlas. Ahora, para su implementación se ha elegido abordar el problema utilizando la metodología UP (Unified Process) [9] para el desarrollo de las fases de iniciación, elaboración, construcción y transición, las cuales permitirán el desarrollo de un software que implemente estas políticas y pueda ser integrado a un navegador Web.

El navegador Web seleccionado para implementar el módulo software que automatizará las políticas y recomendaciones de seguridad es Mozilla Firefox 3.0.8. Para determinar su elección tuvieron en cuenta los siguientes criterios: Uso del navegador y facilidad para estudiar y modificar el código del navegador. Como es ya conocido, Mozilla es un navegador de código libre que permite la modificación de su código y cumple con el segundo criterio; en cuanto al primer criterio se tuvo en cuenta el estudio realizado por Onestat [46].

4.1 FASE DE INICIACIÓN

4.1.1 Presentación del Proyecto

Nombre del proyecto: MVPS for Transacción B2C (Modulo de verificación de Políticas de Seguridad para Transacciones B2C).

Cliente del proyecto: Usuarios de transacciones electrónicas B2C.

Metas del proyecto: El objetivo de este proyecto es crear una extensión, para el navegador Web Mozilla Firefox, que permitirá apoyar en el proceso de transacciones B2C por medio de las políticas y recomendaciones propuestas en el capitulo anterior; verificación de la actualización del navegador, verificación de la identidad de los sitios visitados, verificación de la utilización de conexiones seguras, verificación de la utilización de soporte de seguridad (antivirus, firewall) y recomendaciones generales de seguridad para las transacciones.

4.1.2 Captura de requerimientos

4.1.2.1 Captura de requerimientos, fase cero.

Características del sistema

A continuación se realiza un listado de las características que debe implementar el sistema:

- Verificar las políticas de seguridad mínimas para la realización de transacciones B2C.
    - Verificar la actualización del navegador utilizado.
    - Verificar la identidad de los sitios con los cuales se realizan transacciones B2C.
    - Verificar el tipo de conexión establecido entre el navegador Web y el sitio Web (sitio de comercio B2C).
    - Verificar soporte antivirus y firewall.
- Mostrar el nivel de cumplimiento de las políticas.
- Mostrar detalle de las políticas.
- Mostrar el nivel de seguridad para la transacción.
- Mostrar recomendaciones de acuerdo al nivel de cumplimiento de las políticas.
- Mostrar recomendaciones generales.
- Desplegar alertas de acuerdo a la seguridad en el momento de la transacción.

Contexto del Sistema

a) Modelo del Negocio:

- ***Actores:***

  Usuario Transacción B2C: Es la persona que utiliza un navegador Web, instalado en un computador, para realizar transacciones B2C.

- ***Modelo de Casos de uso del negocio***

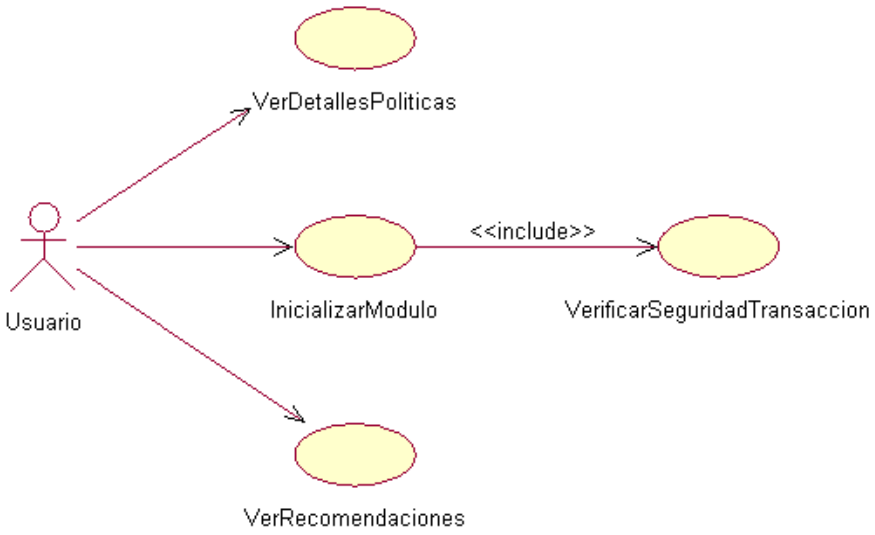

Figura 4.1Modelo de casos de uso del negocio

- ***Casos de Uso del Negocio***

Caso de Uso	Inicializar Módulo
Actores	Usuario transacción B2C
Prioridad	Alta
Descripción	Este caso de uso inicia cuando el usuario activa el módulo MVPS desde la barra de herramientas del navegador Web.

Tabla 4.1 Caso de uso de negocio inicializar modulo

Caso de Uso	Verificar Seguridad Transacción
Actores	Usuario transacción B2C
Prioridad	Alta
Descripción	Este caso de uso inicia cuando el usuario activa el módulo MVPS desde la barra de herramientas del navegador Web.

Tabla 4.2 Caso de uso de negocio verificar seguridad transacción

Caso de Uso	Ver Recomendaciones
Actores	Usuario transacción B2C
Prioridad	Alta
Descripción	Este caso de uso inicia cuando el usuario visualiza una serie de recomendaciones a tener en cuenta para la realización de transacciones electrónicas B2C.

Tabla 4.3 Caso de uso de negocio ver recomendaciones

Caso de Uso	Ver Detalles Políticas
Actores	Usuario transacción B2C
Prioridad	Alta
Descripción	Este caso de uso inicia cuando el usuario activa los detalles de los resultados obtenidos después de verificar cada una de las políticas de seguridad.

Tabla 4.4 Caso de uso de negocio ver detalles políticas

b) Modelo Conceptual

Conceptos: A continuación se presentan una serie de conceptos que serán parte de la aplicación.

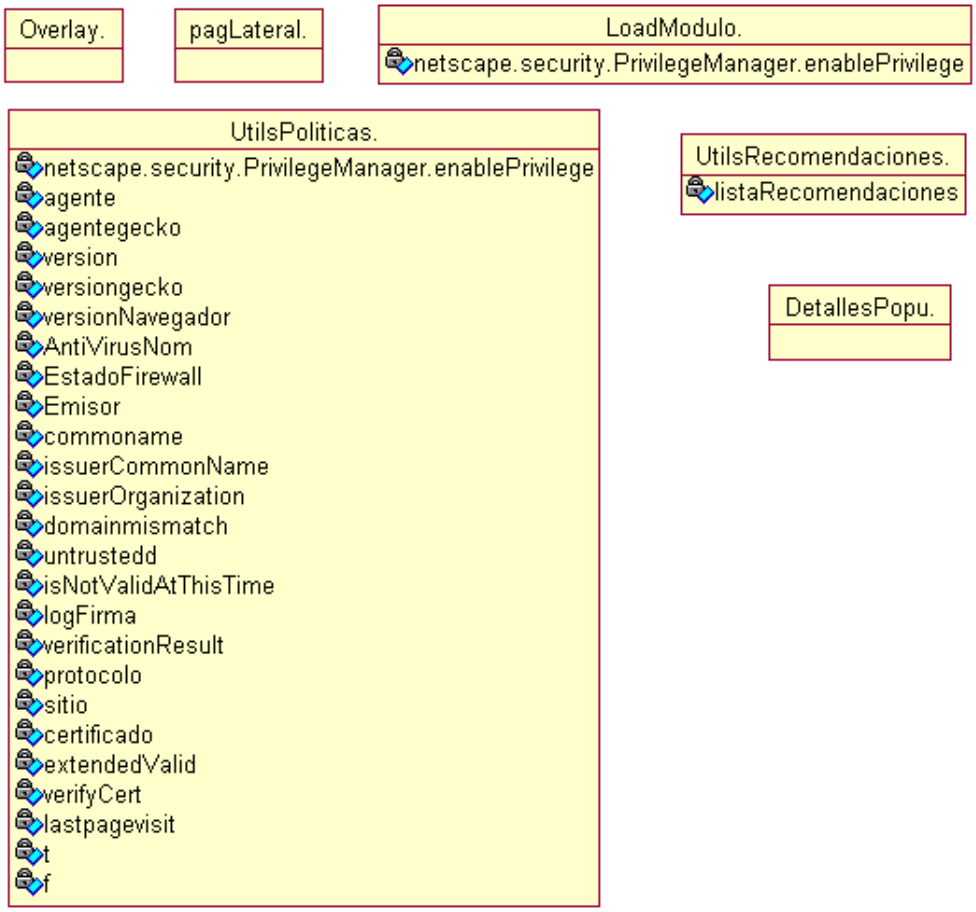

Figura 4.2 Conceptos del sistema

Descripción del Modelo Conceptual: El usuario activa la extensión MPVS por medio de la barra de herramientas del navegador Web. En ese instante el sistema automáticamente se encarga de verificar cada una de las políticas establecidas anteriormente y de tener lista una serie de recomendaciones para transacciones electrónicas de tipo B2C.

Adicionalmente, este módulo se encarga de brindar los detalles de la verificación realizada y de mostrar un nivel de seguridad que presenta el sitio Web visitado por medio del cual se realizará la transacción electrónica.

Listado de las Funciones del sistema

REFERENCIA	*FUNCION*	*CATEGORIA*
R1	**Inicializar Módulo**	
R1.1	*Establecer Valores Iniciales Variables*	*Oculta*
R2	**Verificar Seguridad Transacción**	
R2.1	*Verificar Actualización Navegador*	*Evidente*
R2.2	*Verificar Autenticidad Sitio Web*	*Evidente*
R2.3	*Verificar Nivel Seguridad Conexión*	*Evidente*
R2.4	*Verificar Nivel Seguridad Equipo Local*	*Evidente*
R3	**Ver Recomendaciones**	
R3.1	*Mostrar Recomendaciones Generales*	*Evidente*
R3.2	*Mostrar Recomendaciones Transacción*	*Evidente*
R3.3	*Generar Recomendaciones Transacción*	*Evidente*
R4	***Ver Detalles Políticas***	
R4.1	*Mostrar Detalles de Resultados de las Políticas*	*Oculta*

Tabla 4.5 Listado de funciones del sistema

Requisitos no funcionales

A continuación se especifican las propiedades del sistema tales como: restricciones del entorno, rendimiento, flexibilidad, dependencias con la plataforma, extensibilidad y confiabilidad.

Característica	*Descripción*	*Funciones Afectadas*	*Obligatoria/Opcional*
Sistema Operativo	Windows XP	Todas	Obligatoria
Lenguaje de Programación	HTML, XML, XUL, Java Script C++	Todas	Obligatoria
Persistencia de los datos	El sistema debe mantener la información concerniente a las recomendaciones en archivos planos.	R3.1, R3.2 y R4.1	Opcional
Flexibilidad	El sistema deberá servir de base para la creación de otros sistemas en dominios similares (por ejemplo, para sistemas de transacciones electrónicas B2B)	Todas	Opcional
Tolerancia a fallos	El sistema debe capturar las excepciones que puedan ocurrir cuando se llamen los diferentes métodos de las interfaces	Todas	Obligatoria

Tabla 4.6 Listado de requisitos no funcionales

4.1.2.2 Captura de requerimientos basada en Casos de Uso

Modelo de casos de uso

- **Actores del sistema**

  Usuario Transacción B2C: Es la persona que utiliza un navegador Web, instalado en un computador, para realizar transacciones B2C. Este actor activa el módulo MVPS desde la barra de herramientas del navegador. De este modo la extensión se encarga de verificar cada una de las políticas para el sitio Web que se esté visitando.

- **Casos de Uso**

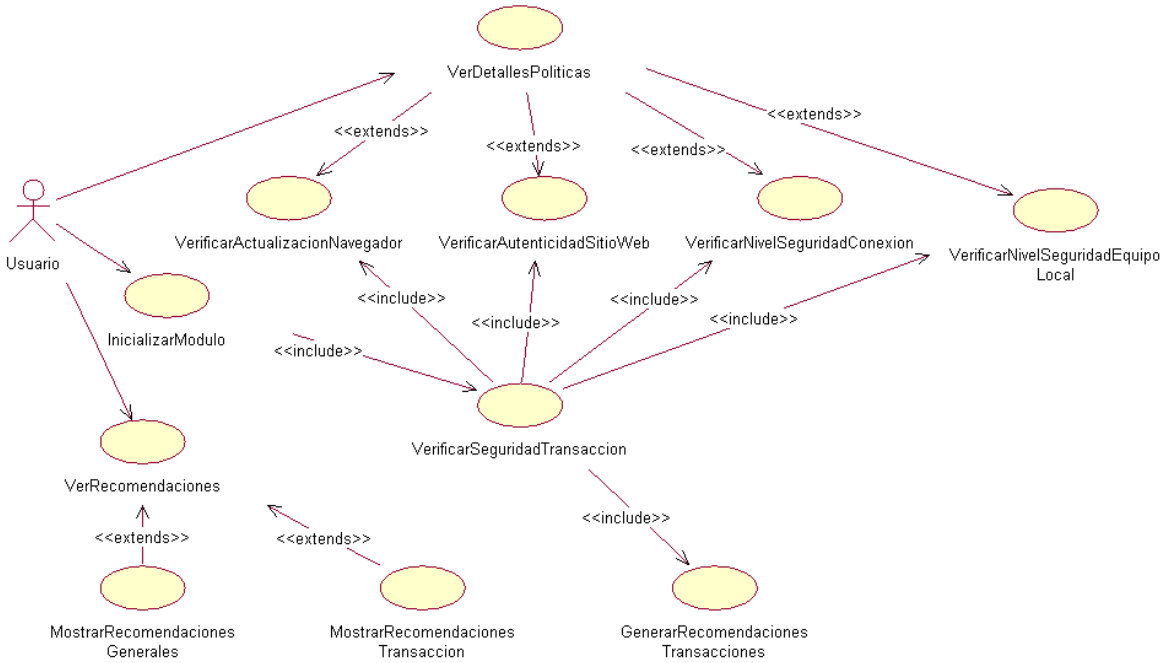

Figura 4.3 Modelo de casos de uso general

- **Descripción resumida de los casos de uso**

Caso de Uso	InicializarModulo
Actores	Usuario transacción B2C
Prioridad	Alta
Referencias cruzadas	R1.1, R2.1, R2.2, R2.3, R2.4
Descripción	Este caso de uso inicia cuando el usuario activa el módulo MVPS desde la barra de herramientas del navegador Web. El sistema al inicializar el módulo establece los valores iniciales de las variables y se encarga de verificar el cumplimiento de las políticas de seguridad establecidas.

Tabla 4.7 Caso de uso inicializar modulo

Caso de Uso	VerificarSeguridadTransaccion
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R2.1, R2.2, R2.3, R2.4
Descripción	Este caso de uso inicia cuando el sistema es activado y se inicializa el módulo. En este caso de uso el sistema verifica las políticas de seguridad implementadas y devuelve un resultado del nivel de seguridad presente en el sitio Web que se está visitando.

Tabla 4.8 Caso de uso verificar seguridad transaccion

Caso de Uso	VerificarActualizacionNavegador
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R2.1
Descripción	Este caso de uso es iniciado por el caso de uso VerificarSeguridadTransaccion y se encarga de verificar la actualización del navegador, última versión.

Tabla 4.9 Caso de uso verificar actualizacion navegador

Caso de Uso	VerificarAutenticidadSitioWeb
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R2.2
Descripción	Este caso de uso es iniciado por el caso de uso VerificarSeguridadTransaccion y se encarga de verificar la identidad del sitio a través de los certificados digitales y la verificación en listas de posibles sitios dedicados a realizar phishing.

Tabla 4.10 Caso de uso verificar autenticidad sitio web

Caso de Uso	VerificarNivelSeguridadConexion
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R2.3
Descripción	Este caso de uso es iniciado por el caso de uso VerificarSeguridadTransaccion y se encarga de verificar los protocolos utilizados para la conexión entre el navegador Web y los sitios de comercio electrónico.

Tabla 4.11 Caso de uso verificar nivel seguridad conexión

Caso de Uso	VerificarNivelSeguridadEquipoLocal
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R2.4
Descripción	Este caso de uso es iniciado por el caso de uso VerificarSeguridadTransaccion y es el encargado de verificar que se encuentre instalado el soporte de seguridad para el navegador; el antivirus se encuentre actualizado, el Firewall esté activo.

Tabla 4.12Caso de uso verificar seguridad equipo local

Caso de Uso	VerRecomendaciones y MostrarRecomendacionesGenerales
Actores	Usuario transacción B2C
Prioridad	Alta
Referencias cruzadas	R3.1
Descripción	Caso de uso que inicia cuando el usuario decide ver las recomendaciones generales para una transacción electrónica brindadas por el sistema.

Tabla 4.13Caso de uso ver recomendaciones y mostrar recomendaciones

Caso de Uso	MostrarRecomendacionesTransaccion
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R3.2
Descripción	Este caso de uso inicia cuando el sistema ha verificado las políticas implementadas y muestra al usuario los resultados del nivel de seguridad encontrados para realizar la transacción electrónica.

Tabla 4.14Caso de uso mostrar recomendaciones transacción

Caso de Uso	Generar Recomendaciones Transacciones
Actores	Sistema
Prioridad	Alta
Referencias cruzadas	R3.3
Descripción	Caso de uso que inicia el sistema después de verificar las políticas y obtener el nivel de seguridad del sitio Web que está visitando. Dependiendo del nivel seguridad el sistema genera una lista de recomendaciones para el usuario.

Tabla 4.15 Caso de uso generar recomendaciones transacción

Caso de Uso	VerDetallesPoliticas
Actores	Usuario transacción B2C
Prioridad	Alta
Referencias cruzadas	R4.1
Descripción	Este caso de uso es iniciado cuando el usuario, después de iniciar el módulo decide visualizar los detalles de cada una de las políticas verificadas.

Tabla 4.16 Caso de uso ver detalles políticas

DIAGRAMAS DE CASOS DE USO ESPECÍFICOS

Caso de uso VerificarActualizacionNavegador

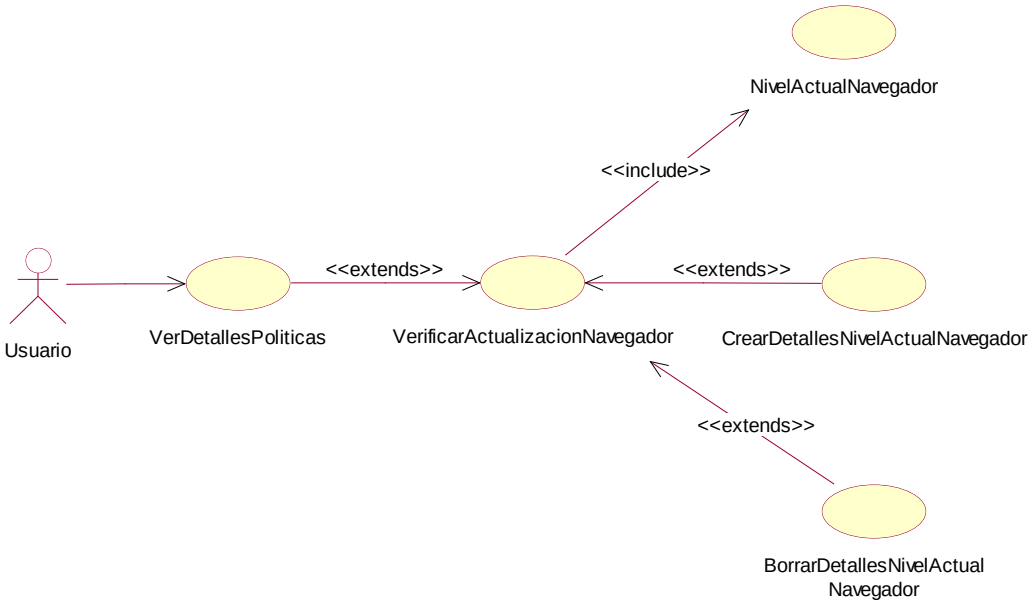

Figura 4.4 Caso de uso verificar actualizacion navegador

Caso de Uso VerificarAutenticidadSitioWeb

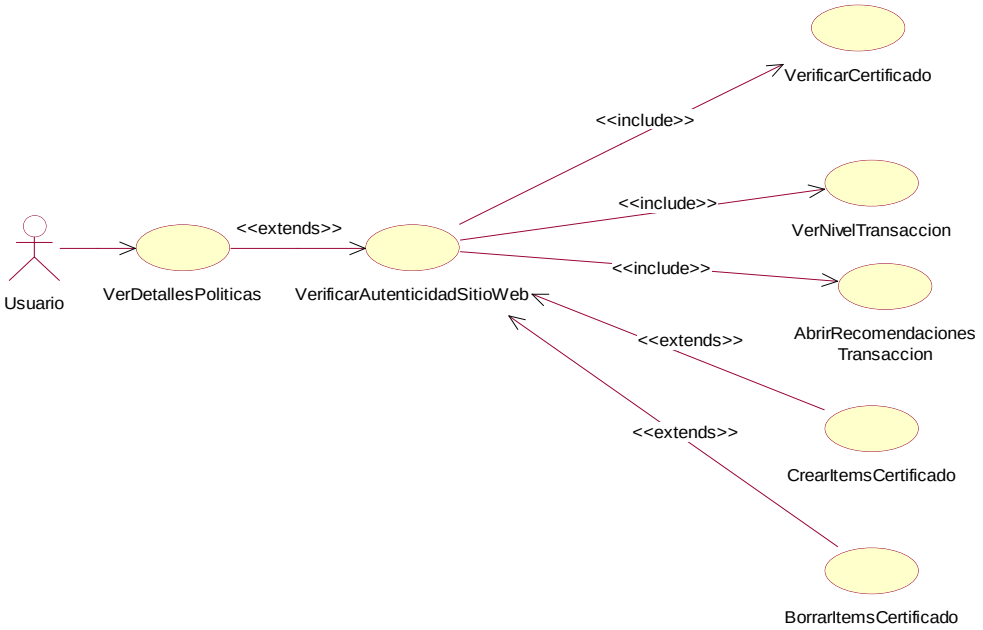

Figura 4.5 Caso de uso verificar autenticidad sitio web

Caso de Uso VerificarNivelSeguridadConexion

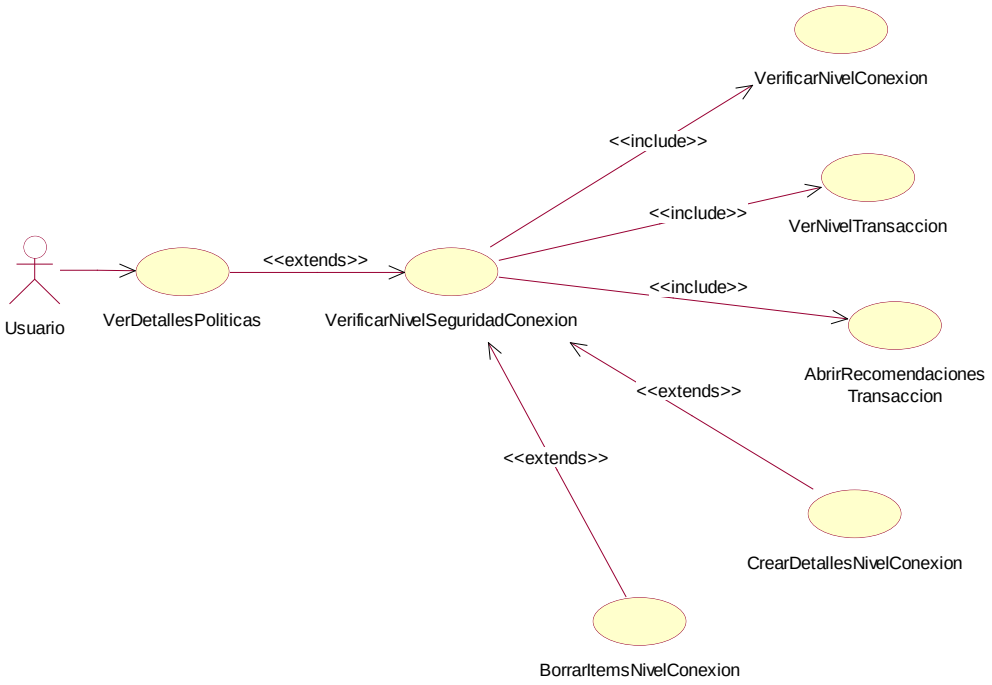

Figura 4.6 Caso de uso verificar nivel seguridad conexion

Caso de uso VerificarNivelSeguridadEquipoLocal

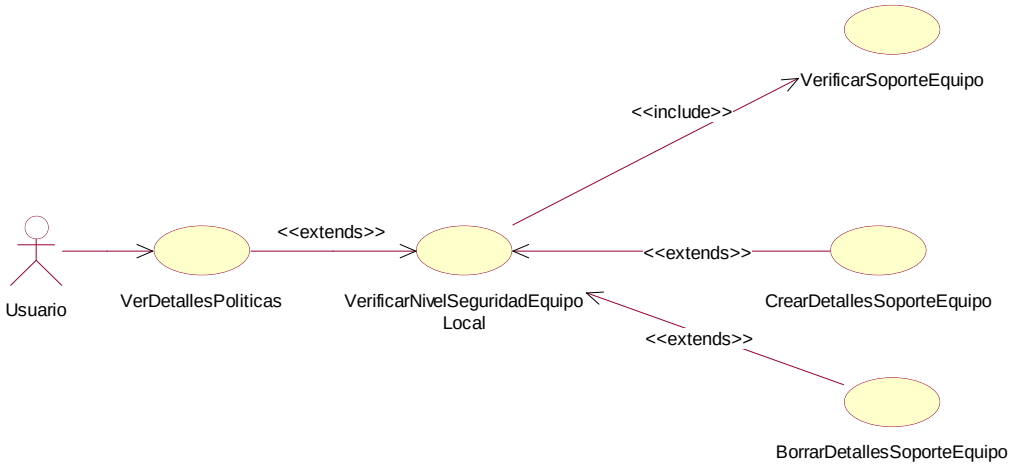

Figura 4.7 Caso de uso verificar nivel seguridad equipo local

Prototipo de interfaces

- **Interface pantalla principal, pestañas Gestión de Seguridad y Recomendaciones Generales.**

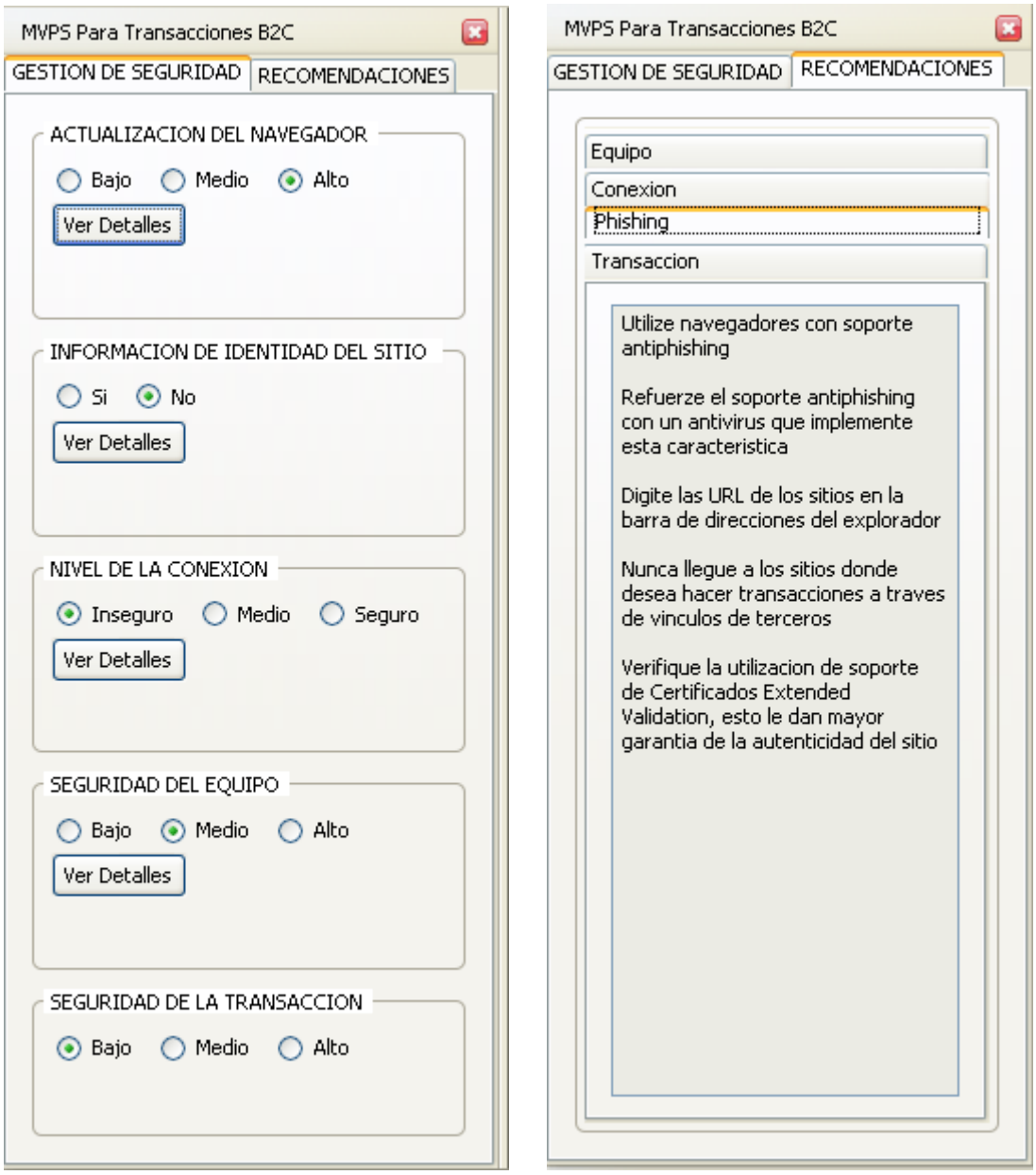

Figura 4.8 Prototipo interface de usuario

El prototipo de la interfaz del módulo MVPS, mostrado en la Figura 4.8, consta de dos pestañas:

- Pestaña de Gestión de Seguridad: En la cual se visualizan los resultados obtenidos por la verificación de cada una de las políticas de seguridad implementadas (etiquetas: actualización del navegador, información de identidad del sitio, nivel de conexión y seguridad del equipo). Adicionalmente, se muestra el nivel de seguridad del sitio dado por el grado de cumplimiento de las políticas (etiqueta: seguridad de la transacción) e información a un nivel de detalle más alto de las políticas verificadas (botones ver detalles).

- Pestaña de Recomendaciones: En la cual se visualizan las recomendaciones de seguridad a nivel general (pestañas equipo, conexión y phishing) y por cada transacción o página Web visitada (pestaña transacción).

4.2 FASE DE ANÁLISIS

Análisis de casos de uso

- **Diagramas de secuencia**

Diagrama de secuencia **InicializarModulo**

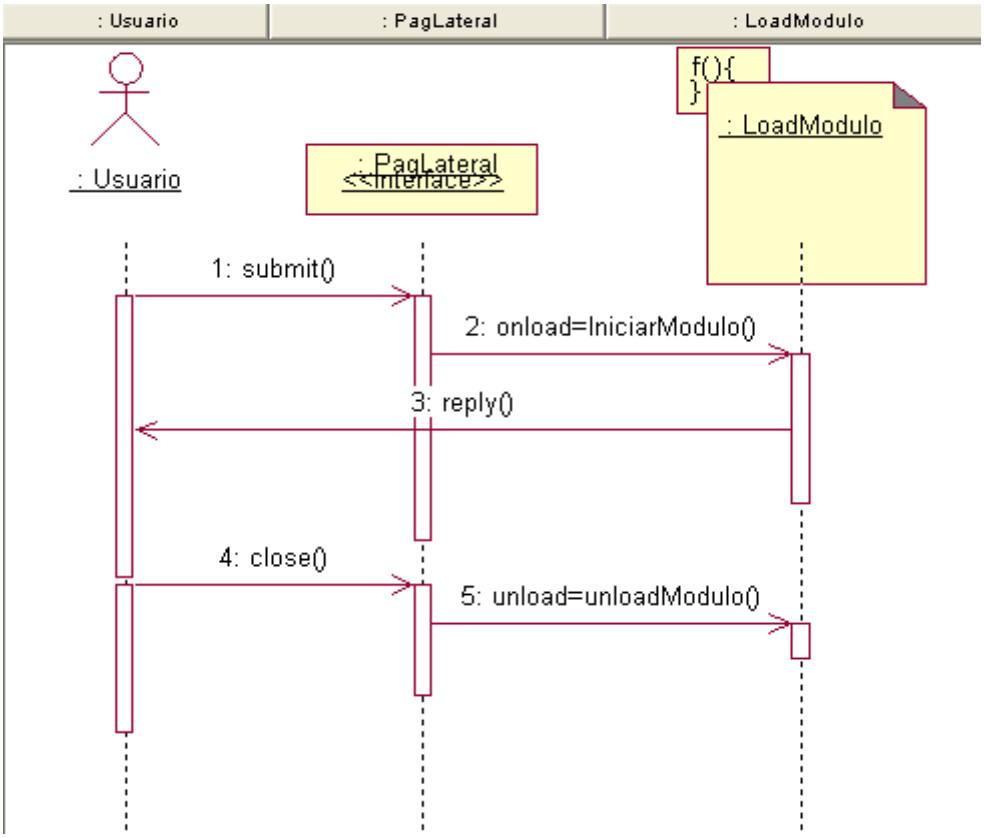

Figura 4.9 Inicializar modulo

El diagrama de secuencia de la Figura 4.9 muestra el curso de eventos que ocurren cuando el usuario inicializa el módulo. El primer paso se da cuando el usuario activa la página lateral; en el segundo paso la página lateral carga e inicializa el módulo, cuyo resultado es mostrar la interfaz de usuario. En los pasos cuatro y cinco cuando el usuario cierra el módulo se liberan recursos.

Diagrama de secuencia **VerificarSeguridadTransaccion**

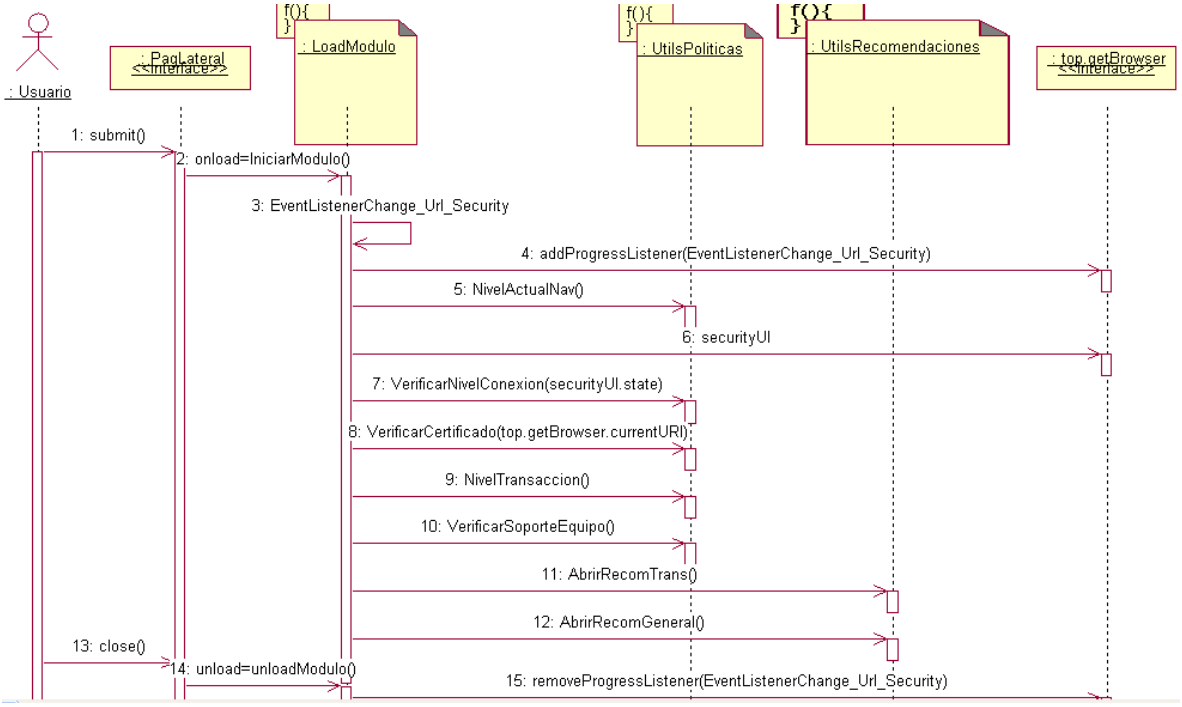

Figura 4.10 Verificar seguridad transacción

El diagrama de secuencia de la Figura 4.10 muestra el curso de eventos que ocurren posteriores a la inicialización del módulo y cuyo objetivo es verificar el nivel de seguridad de la transacción. Para esto, el primer paso es la instancia del elemento EvenListenerChange_Url_Security, el cual es un listener que se pasa como parámetro del evento addProgressListener que se encarga de escuchar los cambios que ocurren en las URL's y cambios de estado de la seguridad del navegador (objeto top.getBrowser). Los pasos siguientes son la verificación de la actualización del navegador (NivelActualNav), verificación del nivel de conexión (VerificarNivelConexion) que tiene como parámetro el objeto securityUI el cual contiene información de seguridad del navegador, verificación del certificado para la URL actual, verificación del soporte equipo (antivirus y firewall) y el establecimiento del nivel de seguridad para la URL actual.

Diagrama de secuencia **VerificarAutenticidadSitioWeb**

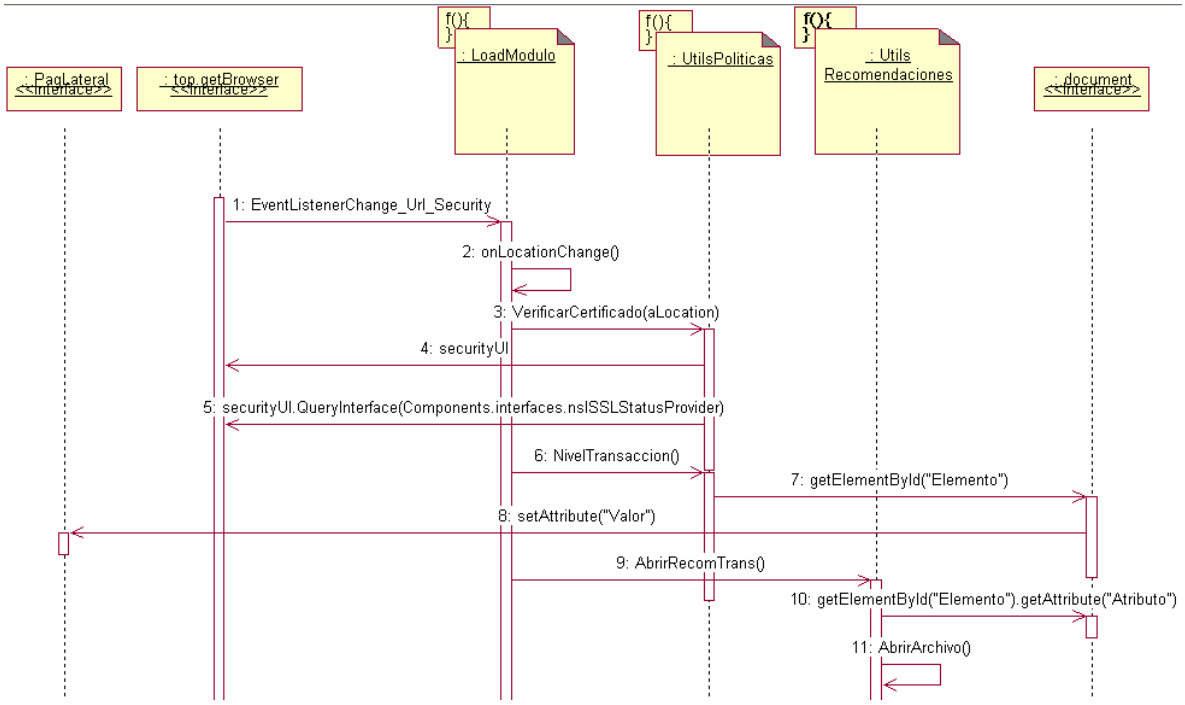

Figura 4.11 Verificar autenticidad sitio web

En el diagrama de la Figura 4.11 se muestra detalladamente la secuencia de eventos de lo que ocurre cuando se verifica la autenticidad del sitio Web que se este visitando. En este caso el listener EventlistenerChange_Url_Security esta en escucha del cambio de URL en el navegador. Cuando esto ocurre se verifica el certificado de la página con el parámetro aLocation; esto se logra recuperando el certificado por medio de la interfaz nsISSLStatusProvider que es un parámetro que se pasa a través del componente de seguridad securityUI.QueryInterface. Los últimos pasos son analizar el nivel de la transacción actual y fijar el elemento para visualizar el uso de un certificado.

Diagrama Secuencia **VerificarNivelSeguridadConexion**

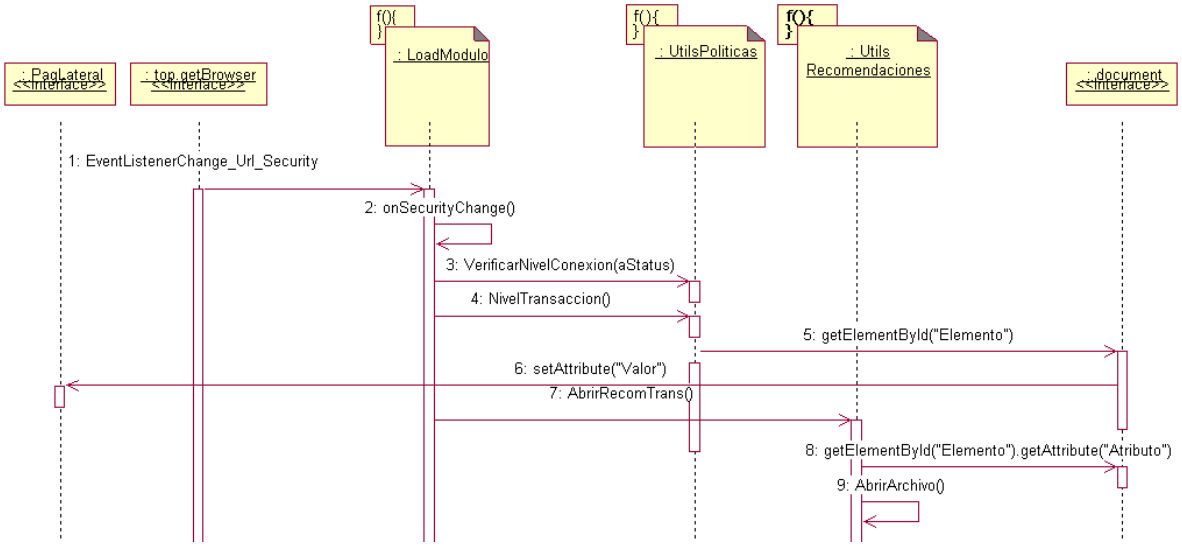

Figura 4.12 Verificar nivel seguridad conexión

En el diagrama de la Figura 4.12 se muestra la secuencia de eventos que ocurren cuando se verifica el nivel de seguridad de la conexión. En este caso el Listener EventlistenerChange_Url_Security esta en escucha del cambio de URL en el navegador. Cuando esto sucede se verifica el estado de la conexión con el parámetro aStatus. Con este parámetro se verifica si la página actual visitada presenta certificados y si este tipo certificados son Extended Validation. Los últimos pasos son analizar el nivel de la conexión actual y fijar el elemento para visualizar el resultado en la interfaz del usuario.

Diagrama secuencia **VerificarSoporteEquipo**

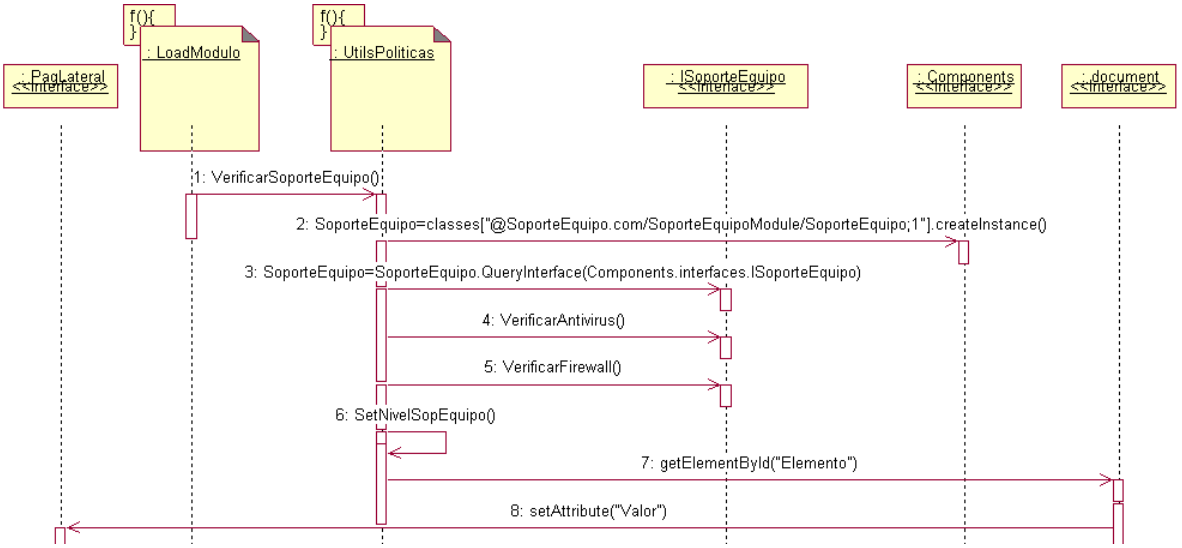

Figura 4.13 Verificar soporte equipo

En la Figura 4.13 se muestra la secuencia de eventos seguida para verificar el soporte del equipo, información del antivirus y Firewall. El primer paso luego de llamar a la función VerificarSoporteEquipo es instanciar el componente SoporteEquipo el cual implementa las funciones que retornan el nombre del antivirus y el estado del Firewall. Por último se fijan los elementos de la interfaz de usuario con la información que retornan las funciones.

Diagrama secuencia **VerDetallesPoliticasActualizacionNavegador**

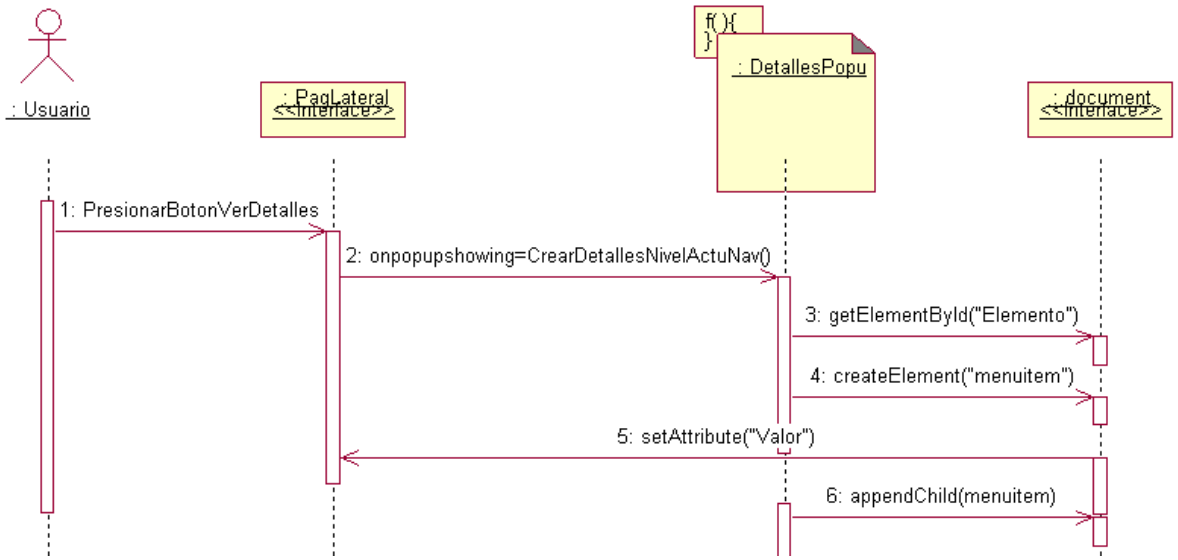

Figura 4.14 Ver detalles de la política de actualización navegador

En el diagrama de la Figura 4.14 se muestra la secuencia de eventos que permite desplegar información de la política que verifica la actualización del navegador. Este proceso se inicia cuando el usuario presiona el botón VerDetalles de la Página Lateral correspondiente a la funcionalidad de actualización del navegador. Cuando se presiona el botón se genera una ventana emergente en la cual se visualiza la información en la interfaz del usuario.

Diagrama secuencia **VerDetallesPoliticasConfianzaSitio**

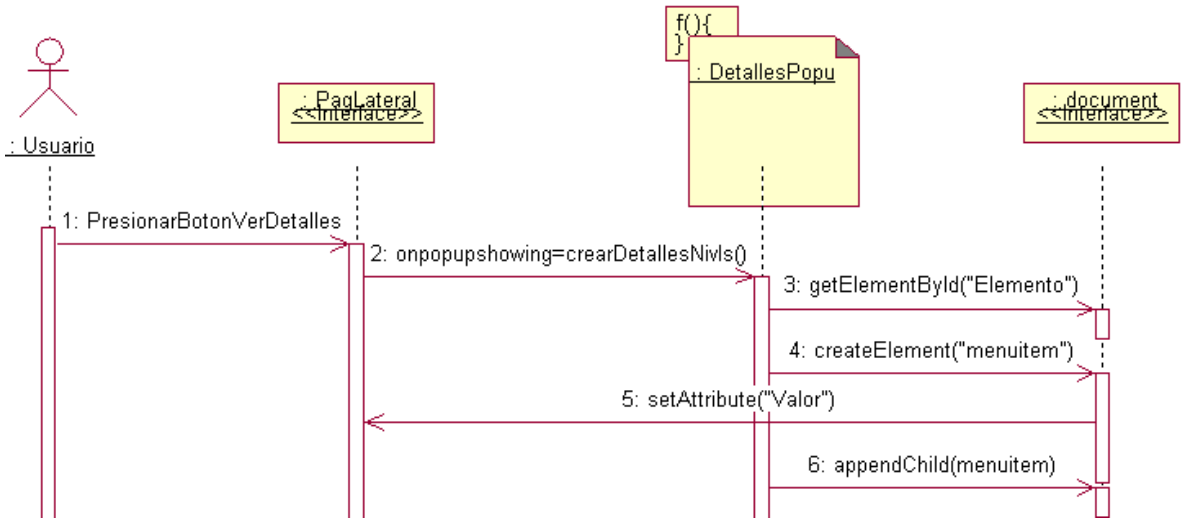

Figura 4.15 Ver detalles políticas confianza sitio

En el diagrama de la Figura 4.15 se muestra detalladamente la información obtenida a partir de la verificación de la política relacionada a la identidad del sitio. Este proceso se inicia cuando el usuario presiona el botón VerDetalles de la Página Lateral correspondiente a la funcionalidad de información de identidad del sitio. Cuando se presiona el botón se genera una ventana emergente en la cual se visualiza la información en la interfaz del usuario.

Diagrama secuencia **VerDetallesPoliticasNivelConexion**

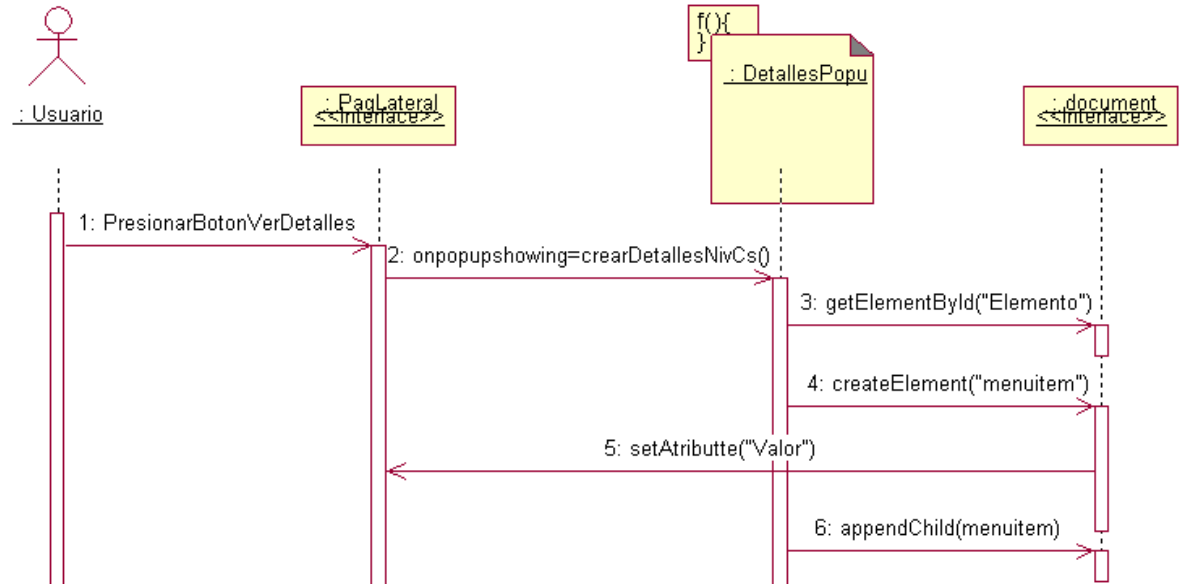

Figura 4.16 Ver detalles políticas nivel conexión

En el diagrama de la Figura 4.16 se muestra detalladamente la información obtenida a partir de la verificación de la política correspondiente al nivel de seguridad de la conexión. Este proceso se inicia cuando el usuario presiona el botón VerDetalles de la Página Lateral correspondiente a la funcionalidad de nivel de conexión. Cuando se presiona el botón se genera una ventana emergente en la cual se visualiza la información en la interfaz del usuario.

Diagrama secuencia **VerDetallesPoliticasSeguridadEquipo**

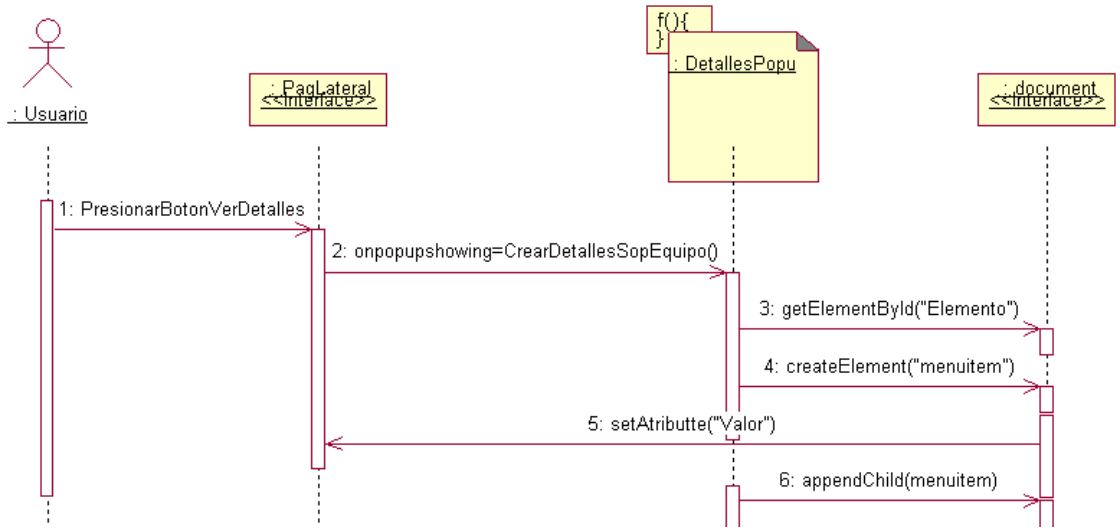

Figura 4.17 Ver detalles políticas seguridad equipo

En el diagrama de la Figura 4.17 se muestra detalladamente la información obtenida a partir de la verificación de la política correspondiente a la seguridad del equipo local. Este proceso se inicia cuando el usuario presiona el botón VerDetalles de la Página Lateral correspondiente a la funcionalidad de verificación del antivirus y del firewall en la máquina local. Cuando se presiona el botón se genera una ventana emergente en la cual se visualiza la información en la interfaz del usuario.

4.3 FASE DE DISEÑO

Diagrama de Componentes

En el siguiente diagrama se muestra cómo se relaciona la extensión MVPS con Mozilla Firefox, mediante un diagrama de paquetes:

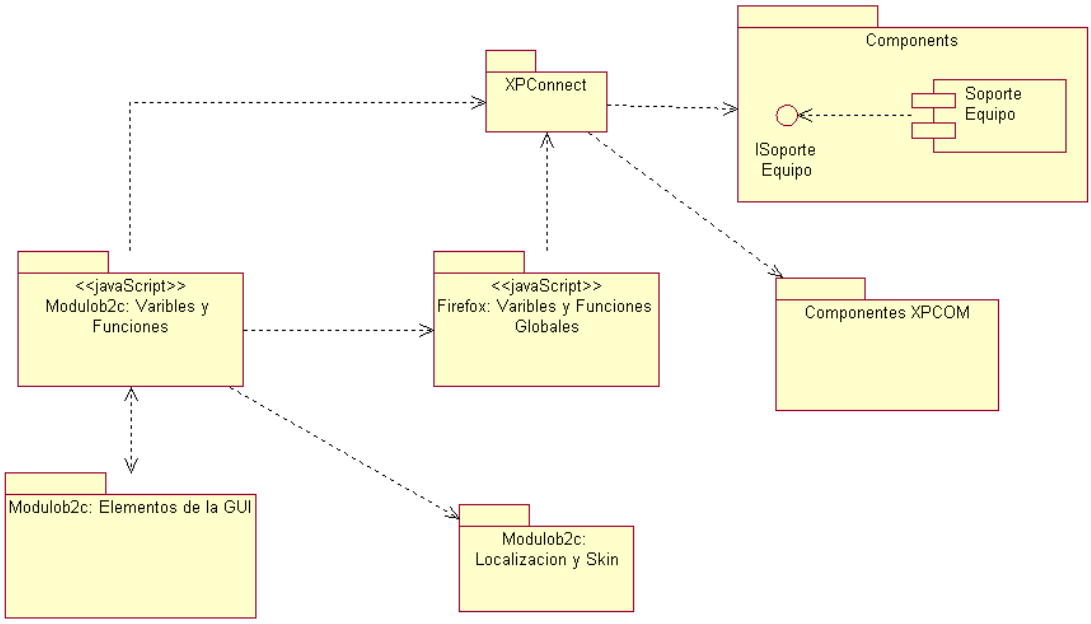

Figura 4.18 Modelo funcional - paquetes del sistema

En el paquete Modulob2c: Variables y Funciones JavaScript se controla el comportamiento de la aplicación, es decir, se implementa la lógica del sistema. Se puede observar que desde ahí se tiene acceso a los elementos de la GUI, así como a los de Localización (para extraer cadenas de texto) y a los Skins (para los elementos como los íconos o imágenes). Las funciones JavaScript también tienen acceso a las funciones y variables definidas globalmente en Mozilla Firefox (Firefox: Variables y Funciones Globales), las cuales controlan una gran cantidad de aspectos de la aplicación, como obtener datos del sistema operativo en el que se encuentra.

La funcionalidad de estas funciones JavaScript se implementa por medio de llamadas a componentes XPCOM. Las propias funciones JavaScript de la extensión también tienen acceso a los componentes XPCOM. (A los componentes XPCOM hay que acceder a través de la capa XPConnect, que es la que ofrece a las funciones JavaScript una interfaz para acceder a estos componentes).

Diseño de la arquitectura

La arquitectura seleccionada para este proyecto es una arquitectura en capas, específicamente de dos capas:

- Capa de presentación
- Capa de lógica

En el siguiente diagrama se presenta dicha arquitectura:

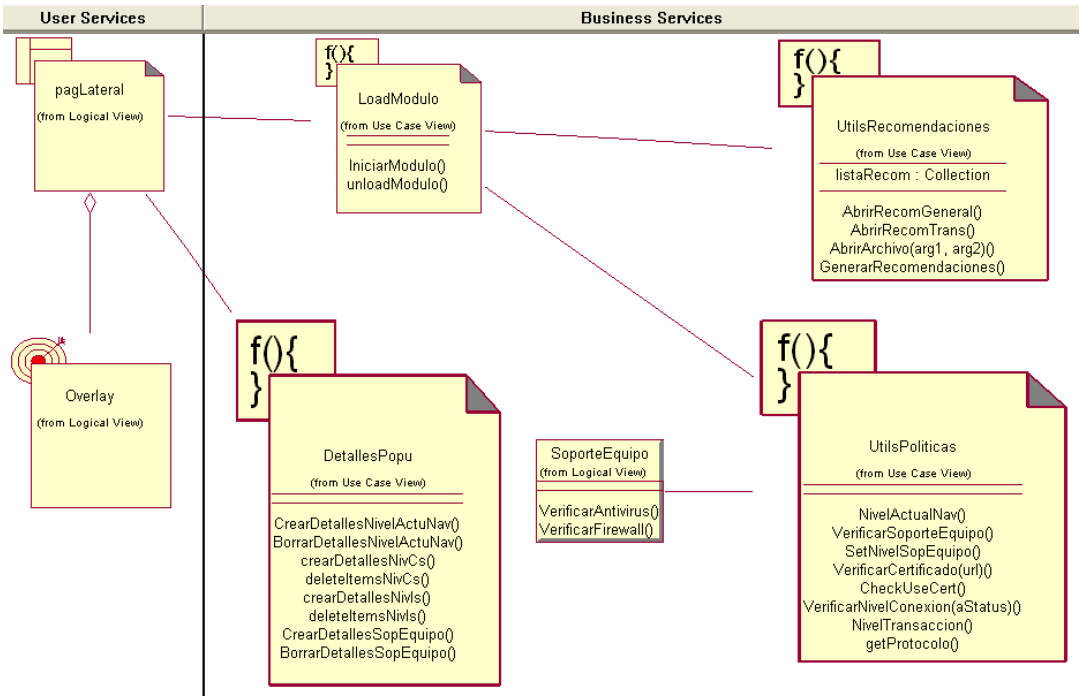

Figura 4.19 Arquitectura del sistema

El módulo MVPS tiene una arquitectura de dos capas (presentación y lógica), debido a que no es necesario el manejo de acceso a datos, y esto gracias a que todos los datos (información del sistema operativo, información de aplicaciones instaladas en la máquina local, cambios en la URL – cambio de página Web), se obtienen por medio de componentes XPCOM del navegador Mozilla Firefox.

La capa de presentación contiene todas las interfaces gráficas que se utilizan en el proyecto para mostrar la información al usuario.

La capa de lógica contiene todas las clases que se encargan de manejar la lógica de negocio de la aplicación. En estas clases se procesan los datos y se obtiene un resultado para el usuario, el cual indica el nivel de seguridad del sitio Web que se está visitando.

Diagrama de Clases

A continuación se presenta el diagrama de clases de la aplicación.

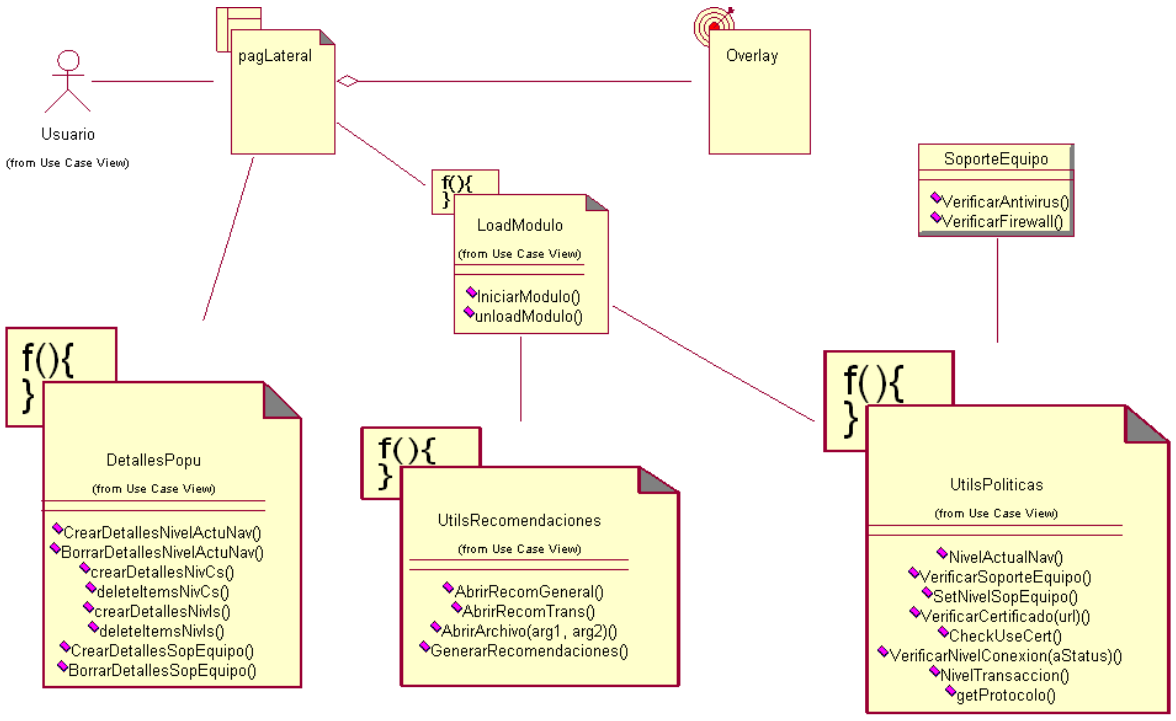

Figura 4.20 Diagrama de clases del sistema

La clase PagLateral es la interfaz gráfica por medio la cual el usuario interactúa con la aplicación. PagLateral muestra el resultado de validar las políticas de seguridad en el sitio Web visitado. Adicionalmente, se presentan al usuario una serie de recomendaciones a tener en cuenta en las transacciones electrónicas.

La clase Overlay sobrepone la interfaz PagLateral en el navegador Web.

El archivo javaScript LoadModulo implementa la clase EventListener la cual está pendiente de los eventos ocurridos en el navegador, tales como cambios en la dirección de la URL o cambio de protocolo de conexión.

La clase UtilsPolíticas implementa acciones como verificar la versión del navegador, verificar la información de identidad del sitio Web y verificar el nivel de la conexión del sitio Web.
La clase UtilsRecomendaciones se encarga de leer de un archivo plano las recomendaciones de seguridad a tener en cuenta por parte del usuario, dependiendo del nivel de seguridad presente en el sitio Web visitado. Adicionalmente, esta clase genera una serie de recomendaciones generales de ayuda para el usuario.

La clase SoporteEquipo implementa los métodos que verifican la seguridad de la máquina local. Se encarga de verificar si el firewall de la máquina local está activado y verificar si se tiene instalado un navegador en la máquina local.

La clase DetallesPopu genera el resultado obtenido, en forma de menú desplegable, después de verificar las políticas de seguridad en el sitio Web visitado.

Estructura física – Distribución de los archivos que conforman la extensión MVPS

A continuación se presenta la estructura de directorios que conforman la extensión MVPS. Esta estructura de directorios es la que ofrece Mozilla Firefox para el desarrollo de extensiones.

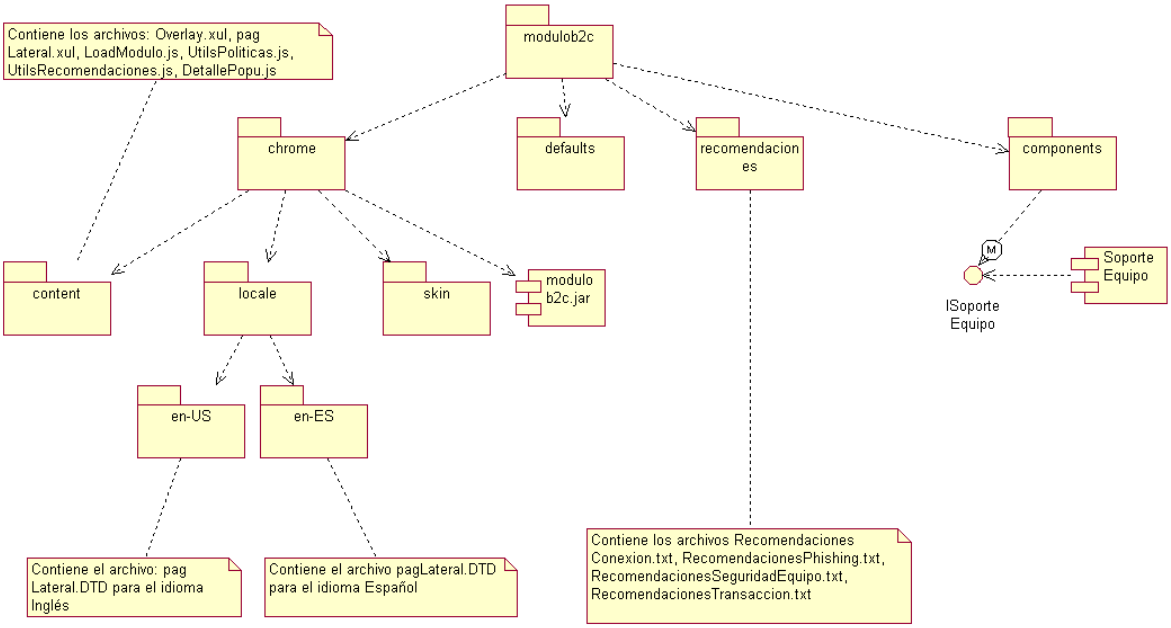

Figura 4.21 Estructura física del modulo

En la Figura 4.21 se muestra la estructura física que Mozilla Firefox establece para la implementación de extensiones [47]. Se establece un directorio chrome en el cual se adicionan los archivos que manejan la lógica de la extensión (directorio content), los archivos de tipo CSS (directorio en-US ó en-ES), archivos para el manejo se skins (directorio skin), archivo .jar que comprime los directorios ya nombrados.

Además, se adiciona un directorio llamado components en el cual se agregan las .dll junto con sus librerías (ver Anexo E, figura 5.7) de tipos que proveen de mayor funcionalidad a la extensión.

Los directorios defaults y recomendaciones son opcionales.

Al final, los directorios de primer nivel (chrome, defaults, recomendaciones, components) se comprimen en un archivo de tipo .xpi el cual luego es llamado desde Mozilla Firefox para realizar el proceso de instalación de la extensión.

El manejar la extensión con esta estructura de directorios permite que modificar o adicionar nuevas políticas requiera de cambios muy puntuales dentro de la estructura de directorios, en primer lugar si se quisiera adicionar una nueva política existe un componente principal que se encarga de escuchar los eventos mas importantes del navegador: cambios de url y cambios de estado de seguridad (ver Anexo E, figura 4.9). Desde esta parte se pueden llamar nueva funcionalidad implementada en componentes XPCOM o java script, de igual forma la interface de usuario esta pensada para adicionar nuevos elementos sin tanto traumatismo de la ya existente.

4.4 FASE DE IMPLEMENTACIÓN

Las políticas ha implementar deben ser utilizadas por usuarios de transacciones B2C, por comodidad para estos se decidió automatizarlas y dejar que sea el propio navegador quien las ejecute. La implementación en el navegador se da gracias a el lenguaje de programación XUL(ver Anexo D) entonces para extender Firefox con las nuevas políticas o cualquier otro producto de la suite de Mozilla lo primero que hay que hacer es crear las interfaces necesarias en XUL, y posteriormente darle dinamismo por medio de Java Script, pues es a través de este que se da la funcionalidad necesaria para agregar contenido dinámico a las aplicaciones y permitir instanciar componentes o acceder servicios del Framework de Mozilla para ser utilizados en nuestras aplicaciones, además se debe tener en cuenta que el Scripting en Mozilla se puede desarrollar desde tres niveles: uno es el nivel de interface de usuario, en el cual se puede manipular contenido a través del DOM, un nivel para el cliente desde el cual se pueden acceder los servicios de XPCOM (ver Anexo E) y finalmente el nivel de aplicación desde la cual se pueden crear componentes.

Desarrollar componentes XPCOM en C++ tiene la ventaja que se puede acceder todos los componentes del Framework, librerías de terceros, se permite mayor seguridad al encapsular el componente y permitir su acceso solo a través de interfaces, contrario a lo que ocurre con el desarrollo o acceso de componentes desde el nivel aplicación o del cliente respectivamente, desde donde solo se pueden acceder aquellos componentes que han sido definidos para ser accesibles desde Java Script.

Todo lo referente a esta etapa se detalla en el Anexo E y D correspondiente a la implementación del módulo MVPS.

5 PRUEBAS DEL MÓDULO DE VERFICACIÓN DE POLÍTICAS DE SEGURIDAD PARA TRANSACCIONES B2C (MVPS)

Después de realizado el desarrollo del Módulo de Verificación de Políticas de Seguridad para transacciones electrónicas B2C (MVPS), se establece un ambiente de prueba con el fin de probar y validar el software construido y así asegurar la calidad de la aplicación.

Una estrategia de prueba del software debe incluir pruebas de bajo nivel que verifiquen que todos los pequeños segmentos de código fuente se han implementado correctamente, así como pruebas de alto nivel que validen las principales funciones del sistema frente a los requisitos del negocio [48]. A partir de esto, el software se probará desde dos perspectivas diferentes:

1. La lógica interna del programa que comprobará utilizando técnicas de diseño de casos de prueba de caja blanca. Las cuales se detallarán en el Anexo F correspondiente a las pruebas.
2. Los requisitos del software se comprueban utilizando técnicas de diseño de casos de prueba de caja negra.

Las pruebas realizadas, deben tener las siguientes características:

- Una buena prueba tiene una alta probabilidad de encontrar un error.
- Una buena prueba no debe ser redundante. Es decir, no debe existir un motivo por el cual se deba realizar una prueba que tenga el mismo propósito que otra.
- Una buena prueba no debería ser ni demasiado sencilla ni demasiado compleja.

En el Anexo F correspondiente a las pruebas se presenta una descripción detallada de los tipos de pruebas a implementar.

Para las pruebas de caja blanca se obtienen todos los caminos linealmente independientes de la estructura de control del programa, esto se realiza por medio de la Prueba de Camino Básico [48](ver Anexo F, sección 6.2.1). Con las pruebas de caja negra se obtendrá un enfoque complementario que permitirá obtener conjuntos de condiciones de entrada que ejerciten completamente todos los requisitos funcionales del sistema. Por tal razón ambos tipos de pruebas se realizarán en conjunto.

Se debe tener en cuenta cierta información referente al equipo en el cual se realizaron las pruebas, de tal manera que esta información ayude a verificar el correcto funcionamiento del sistema y se pueda comprobar la veracidad de los resultados obtenidos. Por ello, en las siguientes figuras se muestra dicha información.

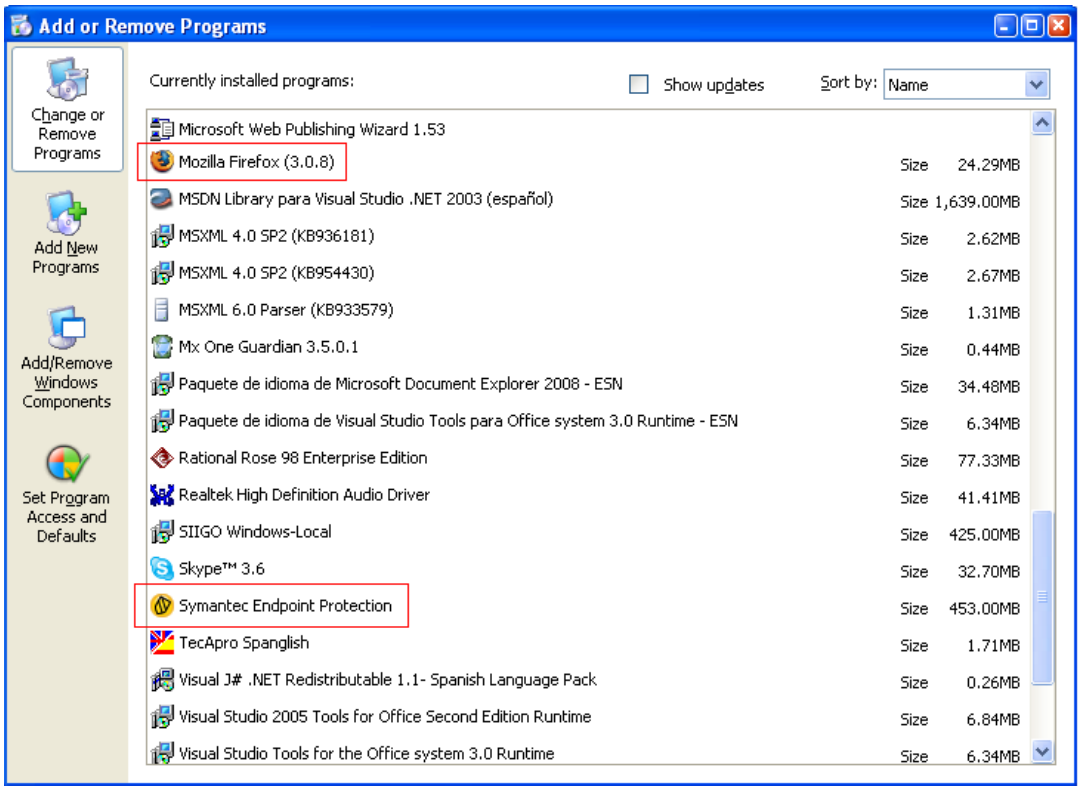

Figura 5.1 Antivirus y navegador Mozilla Firefox instalado en el equipo de prueba

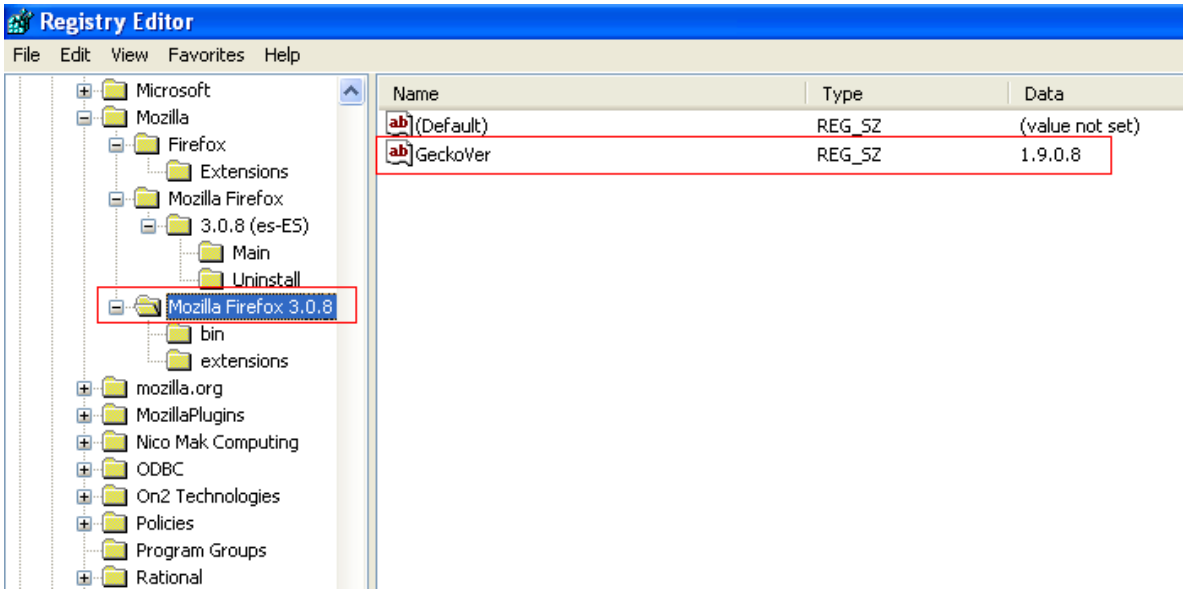

Figura 5.2 Versiones de Mozilla Firefox y del Gecko instalado en la máquina

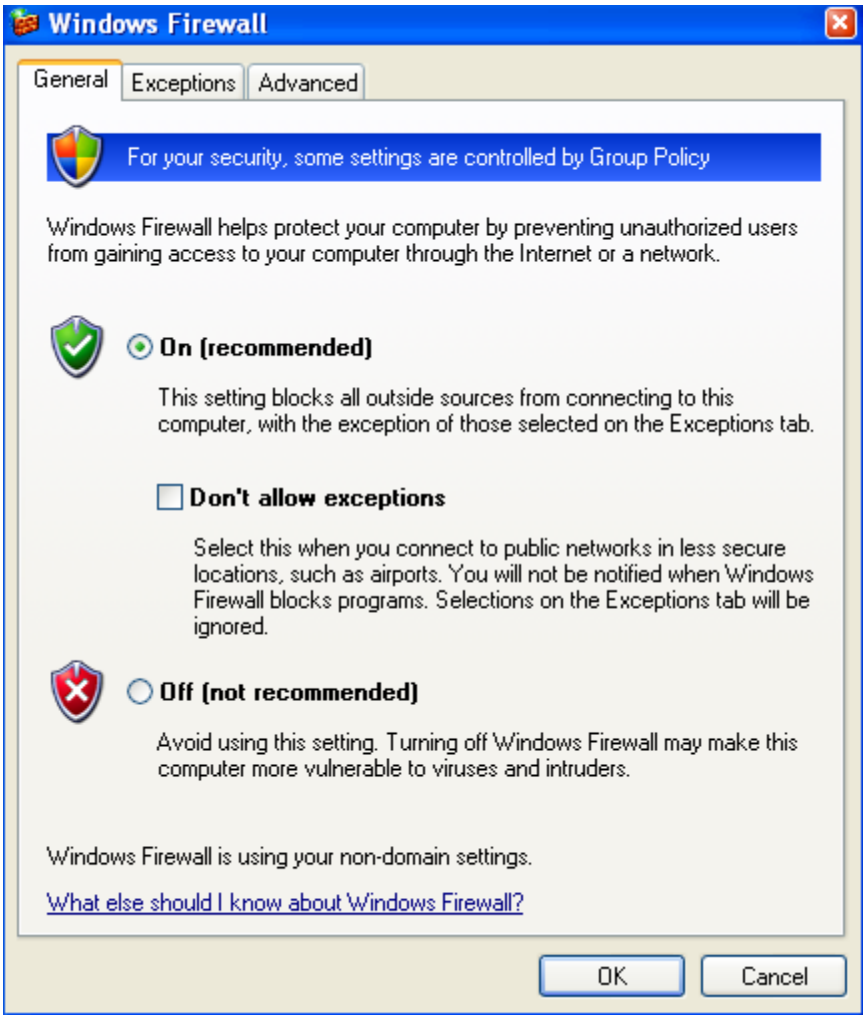

Figura 5.3 Estado del Firewall del sistema operativo

A continuación se describen las diferentes funcionalidades que el módulo MVPS presenta, las cuales se pueden tomar de la Tabla 4.5:

Inicialización del Módulo

En esta funcionalidad de MVPS se establecen los valores iníciales del sistema.
En el momento en que se carga el módulo desde la barra de herramientas (Ver manual de usuario Anexo G), este se encarga de verificar las políticas de seguridad en el sitio en el cual se encuentre cargado en el navegador.

Verificar Actualización del Navegador

En esta funcionalidad se verifica el tipo de navegador y el Gecko instalados en la máquina local en la cual se encuentra el módulo. Adicionalmente se obtiene la versión de estos programas.

Verificar Autenticidad Sitio Web

El módulo se encarga de verificar información del sitio Web en el cual se encuentra actualmente el usuario. Verifica información como dirección electrónica real del sitio Web visitado, validación de existencia de Certificado Extended Validation, Verificación del estado del certificado, nombre real del sitio y nombre de la organización que expide el certificado digital.

Verificar Nivel Seguridad Conexión

En esta funcionalidad, el módulo verifica información sobre el tipo de algoritmo de cifrado utilizado para la conexión, se valida el tipo de conexión (segura o insegura), se verifica el protocolo establecido para la conexión.

Verificar Nivel de Seguridad Equipo Local

El módulo verifica información sobre la seguridad de la máquina local, para esto valida el antivirus instalado y valida si el firewall del sistema operativo se encuentra activado.

Mostrar detalles de resultados de las políticas

El módulo despliega la información detallada de los resultados obtenidos en la verificación de cada una de las políticas anteriores.

Mostrar recomendaciones generales

En esta funcionalidad el módulo carga un conjunto recomendaciones de seguridad para que el usuario tenga en cuenta en el momento de realizar una transacción electrónica.

El ambiente de prueba será conformado con el conjunto de sitios Web que a continuación se presentan, los cuales permitirán verificar[21] y validar[22] el software construido.

Los sitios elegidos para las pruebas son sitios en los cuales se solicitan datos confidenciales de los usuarios de comercio electrónico, tales como: sitios de bancos, sitios de comercio electrónico B2C como (mercado libre, e-bay, amazon), sitios que posean certificados digitales y sitios que no los posean.

Sitios Web de prueba en los cuales se solicita información confidencial de los usuarios:

- Sitios Web de bancos [49][49].

[21] La *verificación* se refiere al conjunto de actividades que aseguran que el software implementa correctamente una función específica. Responde a la siguiente pregunta: ¿Estamos construyendo del producto correctamente?

[22] La *validación* se refiere a un conjunto diferente de actividades que aseguran que el software construido se ajusta a los requisitos del negocio. Responde a la siguiente pregunta: ¿Estamos construyendo el producto correcto?

Caso de prueba para la funcionalidad de Inicialización del Módulo:

Este caso de prueba se permite verificar que el sistema establece correctamente los valores iniciales.
Esta funcionalidad se encarga de cargar el sistema y en este mismo proceso se verifican todas las políticas de seguridad por primera vez.

En las Figuras. 6.1 y 6.2 del Anexo F, se puede verificar que al inicializar el módulo se verifican cada una de las políticas de seguridad.
A continuación se puede observar la verificación de cada una de las políticas de seguridad propuestas.

Caso para Verificación Actualización del navegador: En este caso de prueba de Interfaz se puede verificar que el sistema retorna correctamente la información respecto a la versión del navegador y a la versión del Gecko. Esto se puede observar comparando los resultados de la Figura 5.2 y la información mostrada en la Figura 5.4.

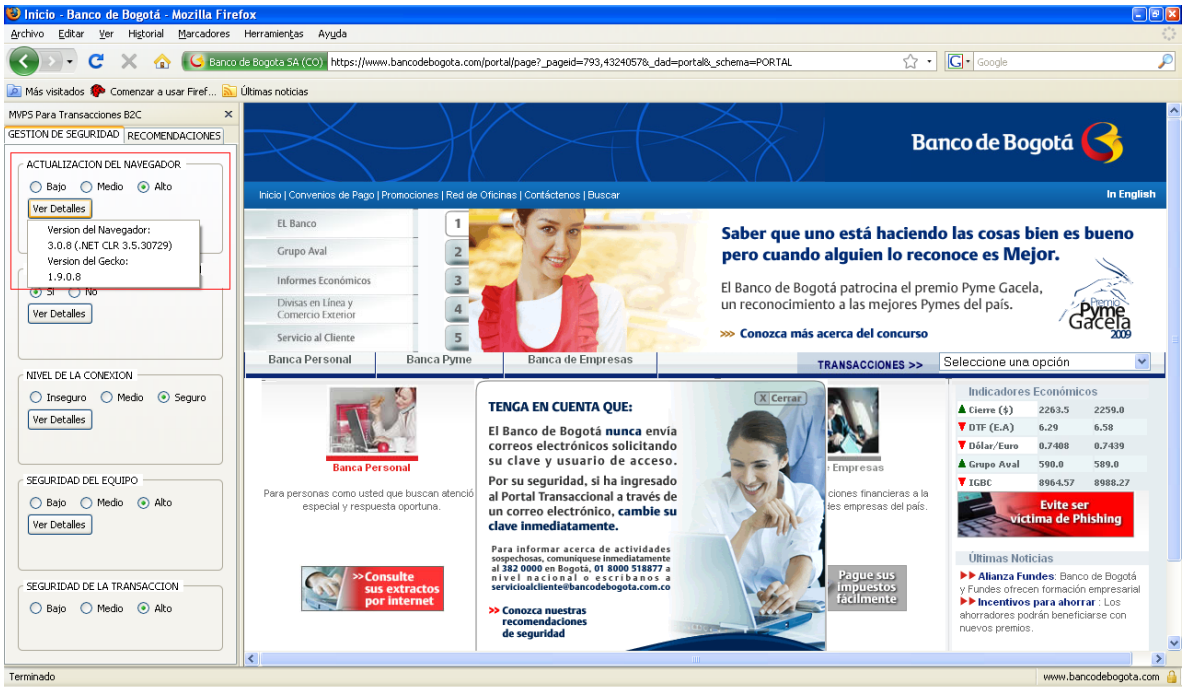

Figura 5.4 Verificación actualización del navegador

En cuanto a la prueba de caja blanca (en el Anexo F, Figura 6.3 y 6. 4) se comprueba que para este caso de prueba el sistema recorre todas las líneas de código que verifican la política de la versión del navegador.

Caso para Verificar Autenticidad Sitio Web: En la Figura 5.5, en cuanto a la prueba de caja negra se puede observar que el sistema arroja los resultados esperados.

Primero, la dirección real del sitio Web visitado coincide con la dirección que muestra el módulo MVPS.

Segundo, el módulo dice que si existe Certificado Extended Validation y esto se comprueba en la URL del navegador (ver sección 1.1.3.3).

Tercero, el sistema muestra el estado del certificado, en caso de que este certificado exista. Este estado puede ser:

- "OK", valor para el cual el certificado es correcto.
- "Sin Verificar" para cuando no se puede verificar el certificado.
- "Revocado" cuando el certificado ya fue revocado.
- "Ha Expirado" en donde el certificado ha expirado.
- "No confiable" cuando el certificado no es confiable.
- "Issuer no confiable" cuando la entidad que firma el certificado no es confiable.
- "Issuer desconocido" cuando la entidad que firma el certificado es desconocida.
- "CA Invalidad" cuando la entidad certificadora que expide el certificado no es válida.
- "Uso no permitido" cuando el certificado se utiliza incorrectamente).

En cuarto lugar MVPS verifica, en caso de que el certificado exista, la entidad que expide el certificado.
En el tercer y cuarto ítem se puede comparar la información que arroja el módulo con la información que brinda la barra de direcciones del navegador (parte izquierda del navegador de color verde para designar que la pagina tiene un certificado extended validation).

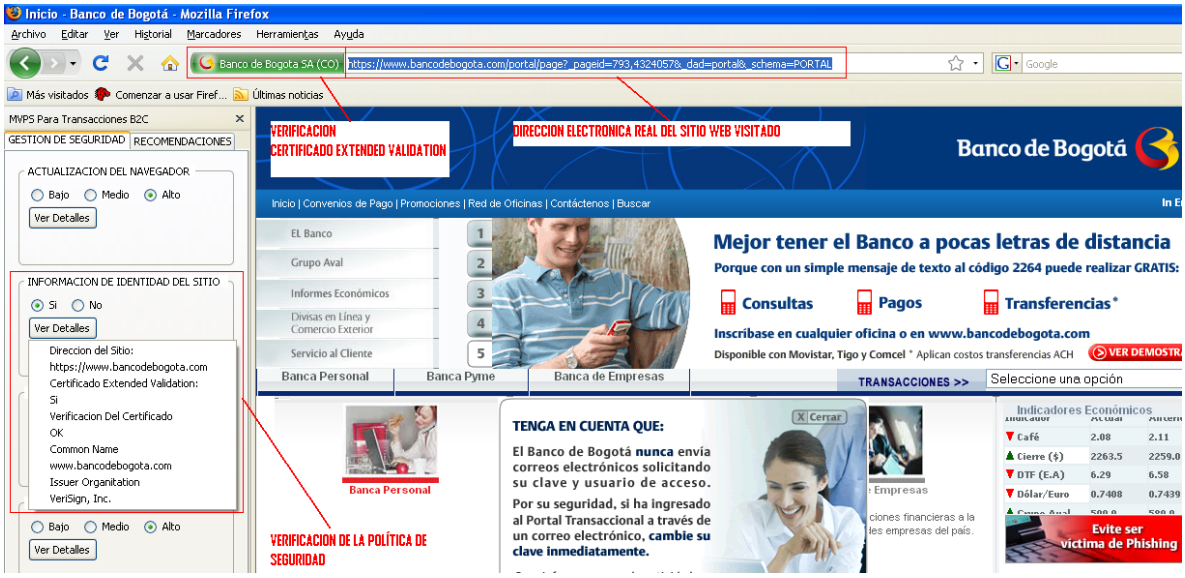

Figura 5.5 Verificar información de identidad del sitio

Las pruebas de caja blanca para este caso de prueba se realizo en el Anexo F (figuras 6.7 y 6. 8). En este tipo de prueba se comprobó cada una de las líneas de código de las funciones que se encargan de probar la política de Verificar la Autenticidad del Sitio Web.

Caso para Verificar Nivel Seguridad Conexión: En la Figura 5.6 se puede observar que el módulo MVPS muestra los resultados correctos, ya que se comparan con los que arroja la opción de información de la página que presenta el navegador.
Tanto en el módulo como en la información de la página se obtienen el mismo tipo de algoritmo de cifrado y la cantidad de bits utilizada por el algoritmo para el cifrado de la llave. MVPS adicionalmente muestra el tipo de protocolo utilizado para la conexión y determina si la conexión es segura o insegura.
Cuando el algoritmo utiliza una cifrado de 128 bits o superior, se considera un nivel de cifrado seguro (ver sección 1.1.3.4)

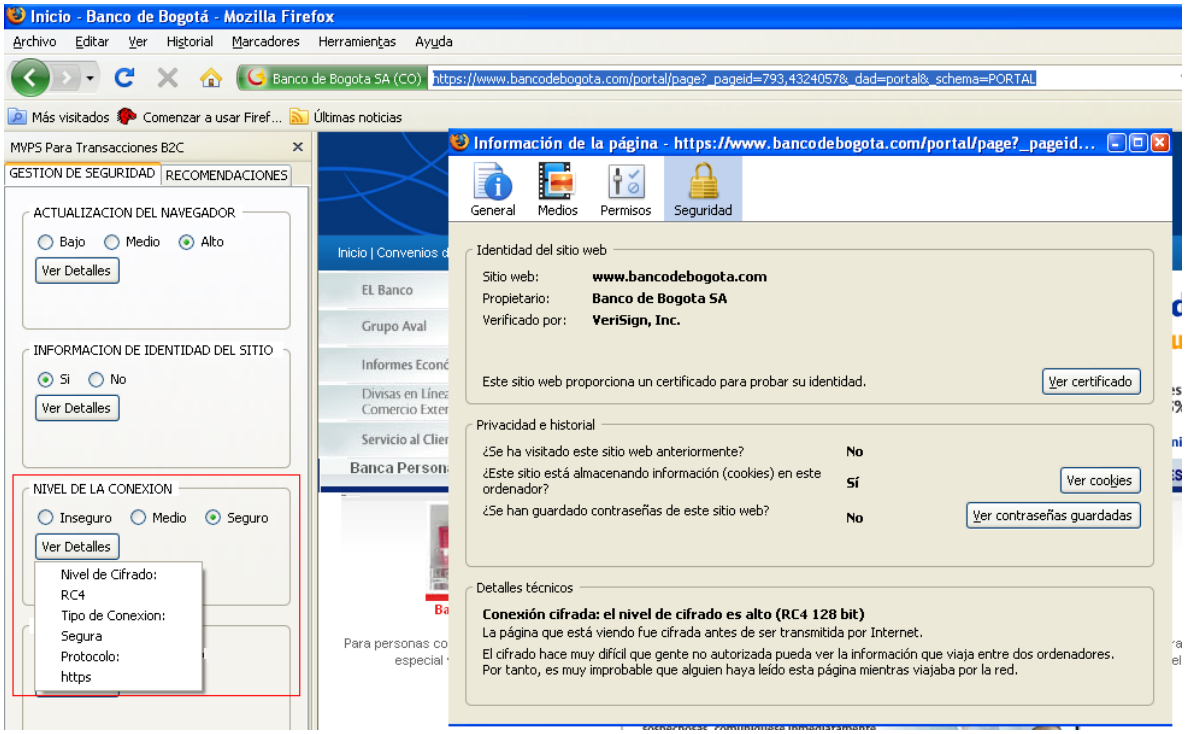

Figura 5.6 Verificación del nivel de conexión

Las pruebas de caja blanca para la política de Verificar nivel seguridad conexión se pueden observar en las Figuras 6.5 y 6.6 del Anexo F. Con las pruebas realizadas se recorrieron cada uno de los caminos del grafo de flujo que se compone de cada una de las sentencias de código que componen la funcionalidad de esta política. Se recorren cada una de las sentencias de código y se puede comprobar que se obtienen los resultados esperados los cuales son visualizados en la prueba de caja negra.

Caso para Verificar Nivel de Seguridad del Equipo Local: En la Figura 5.7 se muestra el resultado que arroja la política que se encarga del equipo en el cual se encuentra instalado el módulo MVPS.

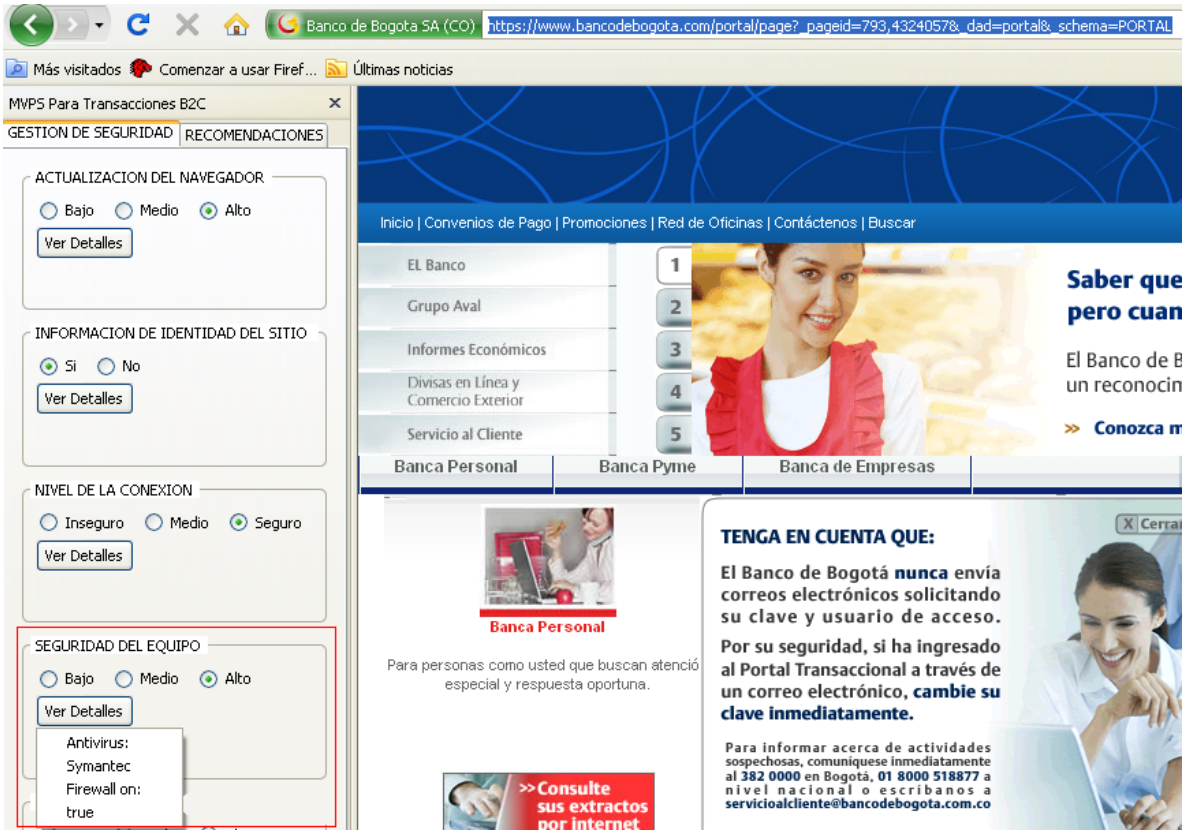

Figura 5.7 Verificar seguridad del equipo

Se comprueba que el resultado obtenido por esta política es el correcto. Esto se concluye comparando las Figuras 5.1 y 5.3 con los resultados mostrados en la Figura 5.7.

Finalmente se obtiene el resultado de la verificación de las políticas anteriores. Este resultado final es el nivel de seguridad que presenta la transacción en el sitio Web que se está visitando. Ver Figura 5.8:

Figura 5.8 Resultado de la evaluación de las políticas de seguridad

Para este caso particular el nivel de seguridad para realizar la transacción en el portal del Banco de Bogotá es ALTO, por lo cual el usuario puede realizar su transacción sabiendo que se han cumplido las condiciones de seguridad mínimas que garantizan su seguridad.

Los mismos tipos de pruebas, tanto de caja negra como de caja blanca se realizaron para diferentes tipos de sitios Web, los cuales fueron categorizados de la siguiente manera:

- Sitios Web de bancos: Este tipo de sitios presentan portales a sus clientes en los cuales ellos tienen la posibilidad de realizar transacciones electrónicas, tales como: consultar saldo en la cuenta, realizar transferencias de dinero, pagar recibos, entre otros.
- Sitios Web de comercio electrónico: Este tipo de sitios ofrecen diferentes clases de productos para la compra y venta. Los usuarios tienen la posibilidad de adquirir cualquiera de ellos y realizar el pago de los artículos solicitados por medio de un formulario para la captura de datos.
- Sitios Web de organizaciones que expiden certificados digitales: Este tipo de certificados son ofrecidos para que los dueños de los portales Web se autentiquen ante cualquiera de sus clientes y de esta manera proteger a los clientes de uno de los fraudes más comunes en Internet (phishing).

Al evaluar el módulo MVPS en diferentes sitios Web que entran en las categorías anteriormente nombradas se obtuvieron los siguientes resultados. (Se aclara que los valores en los que se encuentran los resultados de la evaluación de cada una de las políticas son: B - Bajo, M - Medio, A - Alto):

SITIOS WEB	POLÍTICAS EVALUADAS				
	Actualización del Navegador	Identidad del Sitio Web	Nivel de Conexión	Seguridad del Equipo	Seguridad de la Transacción
https://www.santander.com.co/portal/secciones/BSCH/HOME/PERSONAS/seccion_HTML.jsp	A	A	A	A	A
https://www.mercadolibre.com/	A	A	A	A	A
https://signin.ebay.com/ws	A	A	A	A	A
https://www.amazon.com/gp/	A	A	A	A	A
https://ev.globalsign.com/es/	A	A	A	A	A
https://www.verisign.com/ssl/buy-ssl-certificates/index.html	A	A	A	A	A
https://www.unicauca.edu.co/	A	B	M	A	B

Tabla 5.1 Resultados obtenidos

En todas las pruebas realizadas se verificó que los resultados obtenidos son los esperados, por lo cual se comprueba que el módulo MVPS fue implementado correctamente y cumple con los requisitos funcionales originales.

En la Tabla 5.1 se puede observar que la Seguridad de la Transacción es alta para los sitios Web que entran en la categoría de bancos y de comercio electrónico, al igual que para las entidades emisoras de certificados conocidas.

En la prueba con el portal de la Universidad del Cauca se verifica que le Seguridad de la Conexión es baja, ya que al verificar la identidad del Sitio, se encontró que el certificado que utiliza la Universidad es emitido por una entidad no registrada en la base de datos de certificados del navegador Mozilla.

6 CONCLUSIONES, RECOMENDACIONES Y PROBLEMAS ENCONTRADOS

Este último capítulo tiene por finalidad presentar las conclusiones a las que se llegó una vez culminado este trabajo de investigación, así también plantear una serie de recomendaciones y problemas encontrados encaminadas a ayudar en trabajos futuros que se realicen a partir de los resultados de este proyecto o que estén relacionados con el área de la seguridad en las transacciones electrónicas. Finalmente, se presentan las actividades futuras a llevar a cabo por parte de los investigadores que busquen dar continuidad a la labor iniciada en la presente investigación.

6.1 CONCLUSIONES

La información es uno de los activos más importantes para toda organización, razón por la cual se deben tener los mayores cuidados para que no caiga en manos ajenas. Internet se ha convertido en un medio de intercambio de información que va creciendo de manera acelerada y brinda la posibilidad a todo el mundo de comunicarse muy fácilmente sin la necesidad de salir de la propia casa. Por ende al ser Internet el medio por el cual podemos intercambiar información se deben tener las prevenciones necesarias para que los datos confidenciales no sean hurtados y utilizados de manera inescrupulosa.

A continuación se presentan las conclusiones obtenidas a partir de la elaboración del presente proyecto:

- La utilización de los medios electrónicos, informáticos y telemáticos presentan beneficios evidentes en los usuarios, pero también dan lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de dichos medios. La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) ofrece un método sistemático para analizar los riesgos presentes en los sistemas de información, ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

- La formulación de políticas y recomendaciones de seguridad no deben surgir del azar, se deben seguir estándares y guías para la creación y gestión de las mismas. En el caso particular de este proyecto se utilizó la guía RFC 2196 y el código de prácticas de Seguridad en Gestión de la Información ISO 17799.

- Un sitio Web debe ofrecer una infraestructura de seguridad apropiada para sus usuarios. Esto se logra con la utilización de certificados digitales que provean Extended Validation y a su vez estos certificados sean emitidos por organizaciones reconocidas para este fin. Adicionalmente, se debe tener en cuenta que el canal de conexión utilice un protocolo que implemente algoritmos de cifrado con una llave encriptada de 128 bits o superior.

- El módulo MVPS construido implementa las políticas y recomendaciones de seguridad obtenidas en este proyecto. Para este desarrollo se utilizó componentes XPCOM, debido a que XPCOM está diseñado para ser utilizado a nivel de aplicación.

- El Modelo de Componente Objeto Multiplataforma (XPCOM) permite crear proyectos de forma modular. El proyecto se divide en varias piezas denominadas componentes los cuales son ensamblados en tiempo de ejecución.

- XPCOM permite a diferentes piezas de software ser desarrolladas y construidas independientes unas de otras.

- La interoperabilidad entre componentes de XPCOM se realiza mediante la implementación de interfaces.

- Mozilla Firefox brinda la posibilidad de construir extensiones con el fin de ampliar la funcionalidad de este navegador. Mozilla utiliza el Gecko que es donde el uso de XPCOM se hace más importante, ya que XPCOM se encarga de accesar la funcionalidad de las bibliotecas del Gecko. El módulo MVPS es una extensión creada en esta investigación.

- En general la combinación de las guías, metodologías y tecnologías expuestas en las conclusiones anteriores permitieron la obtención de las políticas y recomendaciones de seguridad propuestas y su automatización por medio del módulo MVPS.

6.2 RECOMENDACIONES

A las personas interesadas en la seguridad de la información se les recomienda profundizar más en el estudio de políticas de seguridad para transacciones electrónicas, con el objetivo de buscar las mejores soluciones para garantizar la seguridad de los datos de los usuarios y de esta forma contribuir al crecimientos del comercio electrónico en la región y en el país.

Por todo el trabajo que involucró el desarrollo del software MVPS y por todos los conocimientos que se tuvieron que aplicar, se puede afirmar que en el proceso de desarrollo de una extensión para el navegador Web Mozilla Firefox se deben complementar muchos de los conceptos tratados en las diferentes asignaturas del programa de Ingeniería de Sistemas de la Universidad del Cauca. Por tal motivo se recomienda integrar las actividades realizadas en asignaturas complementarias, como es el caso de la electiva de Seguridad Computacional y las asignaturas en las que se tratan tópicos relacionados con seguridad de la información, ingeniería del software, desarrollo de aplicaciones Web, entre otros.

De igual manera se recomienda que para proyectos de esta misma índole se pueda contar, no sólo de expertos en seguridad de la información, sino con muchas más personas en diversas áreas, como por ejemplo estudiosos de redes y comercio

electrónico y en general personas que ayuden en la tarea de reforzar los conceptos necesarios para un mejor trabajo respecto al manejo de información confidencial en transacciones por la Web.

Así mismo se recomienda integrar temas relacionados con la seguridad en el comercio electrónico y los aspectos a tener en cuenta en el momento de realizar una transacción a través de Internet, dentro del temario de la electiva seguridad informática del programa de Ingeniería de Sistemas de la Universidad del Cauca.

6.3 PROBLEMAS ENCONTRADOS

En la siguiente tabla se enumeran los problemas encontrados a lo largo del presente proyecto de investigación:

Problemas presentados	Solución
La búsqueda de datos para la realización del análisis de riesgos de forma cuantitativa no fue tarea fácil.	Utilizar herramientas como: PILAR, que permiten calcular la mayoría de datos necesarios para el análisis de riesgos y utilizar fuentes como INTECO, las cuales tienen suficiente información en las cuales se puede apoyar para realizar un análisis cuantitativo.
Creación de instancias de componentes XPCOM desde java script. Por lo general la mala implementación de estos componentes genera excepciones.	Revisar las líneas de código en la cual se instancia el componente. Este problema también puede surgir cuando no se utilizan componentes en estado congelado, la solución es utilizar este tipo de componentes.
Encontrar identificadores de Firefox.	Utilizar la herramienta DomExplorer, la cual genera todo el árbol de directorios del DOM con sus respectivos identificadores.
Implementación del componente principal, el cual debe actuar como escuchador (*listener*) de los procesos y eventos generados por cambios en la URL y cambios de estado de seguridad del navegador.	Implementación de la interface nsIWebProgressListener. Esta interfase posee propiedades y métodos que entregan información referente al estado (*estatus*) de la conexión, URL solicitada, etc.

Retorno de variables desde el componente.	XPCOM gestiona que el llamado y retorno de las funciones se haga con los parámetros adecuados. Para esto utiliza: Primero, la macro NS_IMETHODIMP que es un método que se encarga de retornar y pasar el tipo adecuado. Segundo, nsresult para controlar errores que puedan ocurrir.
	
	Para poder retornar cualquier tipo de dato se debe utilizar el siguiente código:
	
	`*_retval = (char*) nsMemory::Clone(myResult,`
	`sizeof(char)*(strlen(myResult)+1));`
	`return *_retval ? NS_OK :`
	`NS_ERROR_OUT_OF_MEMORY;`
	
	Lo anterior es la forma de controlar el mapeo al tipo dato que se desea retornar.

Creación del archivo nmake para la compilación del componente XPCOM y creación de la DLL.	Existen archivos con este tipo de extensión y que se pueden descargar desde varias páginas. Como recomendación se debe verificar que el archivo está referenciando la misma versión del gecko utilizada.

Registro del componente XPCOM.	*NS_IMPL_NSGETMODULE (SoporteEquipo, components).* Esta es una macro que permite implementar la interfase nsIModule, la cual es utilizada para registrar de forma automática los componentes. Sus parámetros son el nombre con el cual se va a implementar la interfase y una lista que incluye el classname del componente, el identificador de la clase y el identificador del componente. Para poder utilizar la macro se debe incluir el archivo de cabecera nsImodulo.h.
Problemas con librerías de terceros y dependencia de la herramienta Nmake.	No se encontró solución para este problema por lo cual la extensión mantiene su dependencia con la herramienta Nmake.

Tabla 6.1 Problemas encontrados y soluciones propuestas

6.4 TRABAJO FUTURO

El esfuerzo empleado en el desarrollo del Módulo de Verificación de Políticas de Seguridad para Transacciones B2C (MVPS) no debe quedar sólo con lo desarrollado hasta ahora, sino que se debe complementar de tal manera que se pueda ampliar la funcionalidad y las características del módulo, que no se pudieron llevar a cabo en este proyecto debido a los limitantes de tiempo y recursos. Para lograr este fin será necesario buscar organizaciones que apoyen la investigación y el trabajo innovador en nuestro medio.

La funcionalidad y características de MVPS, se puede ampliar con la implementación de recomendaciones y políticas de seguridad que aún no están presentes en el módulo, tales como políticas sobre el manejo de Keyloggers en la máquina local, verificación de actualizaciones del antivirus instalado en la máquina local, verificación del tipo de restricciones configuradas en el firewall, entre otros.

Adicionalmente, sería muy enriquecedor el emprender el desarrollo de una herramienta software similar a MVPS en otros tipos de navegadores. Se podría pensar en crear un módulo con las mismas características que presenta MVPS e inclusive mejorarlas para otros tipos de navegadores. Esto pensando en la diversidad de navegadores que existen y que son mayormente utilizados por la gente.

Con esto se podría avanzar mucho más en cuanto al esquema de seguridad para la información de los usuarios de Internet.

Teniendo en cuenta todas estas recomendaciones se lograría una investigación y aprehensión de conocimientos que redundaría en beneficios personales y en mejora del producto con posibilidades reales de comercialización.

BIBLIOGRAFÍA

[1]. GS1Panamá. *E-commerce: Completo reporte sobre el comercio electrónico en América Latina* (en línea). GS1Panamá: julio 2006 [ref. de 17 de octubre de 2007]. http://www.gs1pa.org/boletin/2006/julio/julio-02.pdf.

[2]. Álvarez, G. *Barreras al Comercio Electrónico*. Instituto para la Seguridad en Internet (en línea). Abril 2007 [ref. de 13 de septiembre de 2007]. http://www.instisec.com/publico/verarticulo.asp?id=47.

[3]. Portaley Las leyes de Internet. *Seguridad en Comercio Electrónico*. Consultoría a abogados en Portaley.com (en línea). [ref. de 7 de agosto de 2007]. http://www.portaley.com/comercio/seguridad-ce.shtml.

[4]. Serrano, C. *Modelo Integral para el Profesional en Ingeniería*. Popayán: Editorial Universidad del Cauca. 2005, pp 56–65

[5]. Ministerio de Administraciones Públicas. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. I – Método, NIPO 326 – 05 – 047 – X. Magerit versión 2 (en línea). Madrid: junio de 2006. 154 p. http://www.csi.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf

[6]. Instituto Argentino de Normalización (IRAM). *Information Technology, code of practice for Information Security Management*. ISO 17799:2005. Segunda Edición. Buenos Aires (Argentina):IRAM, 2002. 82 p.

[7]. Fraser B. *Site Security Handbook*. *RFC 2196* (en línea). Network Working Group. Editorial: SEI/CMU. Septiembre de 1997 [ref. de 2 de febrero de 2008]. http://www.faqs.org/ftp/rfc/pdf/rfc2196.txt.pdf

[8]. Universidad Nacional de Colombia. Vicerrectoria General Dirección Nacional de Informática y Comunicaciones. *Guía para la elaboración de Políticas de Seguridad* (en línea). 2003 [ref. de 5 de febrero de 2008]. 13 p. http://www.unal.edu.co/seguridad/documentos/guia_para_elaborar_politicas_v1_0.pdf

[9]. Jacobson I. & Rumbaugh J. & Booch G. *El Lenguaje Unificado de Modelado. Manual de Referencia.* Madrid: Addison Wesley. 2000. 552 p.

[10]. Doug Turner & Ian Oeschger. *Creating XPCOM Components*. Mozilla.org. 2003 [ref. de 4 de marzo de 2008]. 278 p. http://www.mozilla.org/projects/xpcom/book/cxc/pdf/cxc.pdf

[11]. Jeffrey, R. & Bernard, J. *Comercio Electrónico*. Mc Graw Hill.

[12]. Frias, J. J. *Estudio y desarrollo de la seguridad en el comercio electrónico entre dos entidades productivas a través de Internet* (en línea). Tesis de Grado de Maestría. Instituto Tecnológico y de Estudios Superiores de Monterrey. Monterrey (México): 2000 [ref. de 24 de agosto de 2007]. http://www.geocities.com/jeann_frias/tesis/tesisjfg.pdf

[13]. García, M.E. & Vazquez, R. *Arquitectura de un Billete Electrónico Anónimo*. *Medios Electrónicos de Pago* (en línea). Lab. de Seguridad Informática de SEPI – 2005. 2005 [ref. de 25 de septiembre de 2007]. pp. 71–80. http://www.scielo.cl/scielo.php?pid=S0718-07642005000300010&script=sci_arttext&tlng=en

[14]. Fernández F. & Villalobos D. *Medios de* Pago (en línea). Adarve Corporación Jurídica. FC Editorial. Madrid, [ref. de 5 de junio de 2008]. http://books.google.com.co/books?id=xfVToCWvss4C&pg=PA142&dq=tarjetas+de+credito+y+debito&sig=lyhMPULOIXL4_5_vnYeg7KDrtkI#PPT1,M1

[15]. Álvarez G. *Set a fondo, Secure Electronic Transaction* (en línea). I WORLD La revista de tecnología y estrategia de negocio en Internet. Número 22. [ref. de 5 de marzo de 2008]. http://www.idg.es/iworld/articulo.asp?id=103068&sec=iworld

[16]. Morales J. M. *SSL, Secure Sockets Layer y Otros protocolos seguros para el Comercio Electrónico* (en línea). I edición. Universidad Politécnica de Madrid. 2002 [ref. de 20 de junio de 2008]. 52 p. http://www.moratalaz.jazztel.es/pdfs/ssl.pdf

[17]. Huidrobo Moya J.M. *Sistemas de telecomunicaciones e informáticos: Sistemas Telemáticos* (en línea). Tercera Edición 2005. 206 p. http://books.google.com.co/books?id=mN5wszBGZEsC&pg=PA206&dq=snnifers&sig=YdkPb7NMQECZm90_oUzmzRLltKY#PPP1,M1

[18]. Álvarez G. *Seguridad SSL* (en línea). I WORLD La revista de tecnología y estrategia de negocio en Internet. Número 18. [ref. 5 de marzo de 2008]. http://www.idg.es/iworld/articulo.asp?id=68235&sec=iworld

[19]. Palacios, Rafael. *Introducción a la criptografía: Tipos de Algoritmos* (en línea). Instituto de Investigación Tecnológica. Febrero de 2006 [ref. 7 de agosto de 2008]. 5 p. http://dialnet.unirioja.es/servlet/articulo?codigo=1448365&orden=62875&info=link

[20]. Exchange Server TechCenter. *Descripción de los Certificados Digitales* (en línea). Junio de 2005 [ref. de 5 de febrero de 2008]. http://technet.microsoft.com/es-es/library/bb123848(EXCHG.65).aspx

[21]. VeriSign. *Más de 400 certificados con Extended Validation emitidos* (en línea). Febrero de 2007 [ref 3 de marzo de 2008]. http://www.verisign.es/verisign-inc/page_037122.html

[22]. Martínez Merino M. *Una introducción a la criptografía*. *El criptosistema R.S.A* (en línea). [ref. de 20 de septiembre de 2008].39 p. http://www.ubu.es/ubu/cm/images?idMmedia=41101

[23]. Martorell M. P. *Criptología* (en línea). Escola Universitaria Politécnica de Marató. Departamento de Telecomunicaciones. [ref. de 22 de septiembre de 2008]. 40 p. http://www.tierradelazaro.com/public/libros/cripto.pdf

[24]. Portal del Banco de Bogotá. *Políticas de Seguridad* (en línea). Octubre de 2007 [ref. 27 noviembre de 2007]. http://www.bancodebogota.com.co/portal/page?_pageid=793,4212425&_dad=portal&_schema=PORTAL

[25]. Norton from Symantec. *Una estrategia de seguridad para las transacciones en línea* (en línea). Norton; enero de 2007 [ref. de 30 de noviembre de 2007]. http://www.symantec.com/es/mx/home_homeoffice/library/article.jsp?aid=transaction_security_plan

[26]. Echarri, A. & Guillermo, S. *Google presenta Google Checkout, un nuevo servicio de pago online seguro, rápido y eficaz* (en línea). Centro de prensa Google; junio de 2006 [ref. 1 de diciembre de 2007]. http://www.google.com/intl/es/press/pressrel/checkout.html

[27]. Peha, J.M. & Khamitov, I.M. *Pay Cash: A Secure Efficient Internet Payment System* (en línea). Proceeding of the 5th International Conference on Electronic Commerce ICEC'03 Publisher. [ref. de 3 de julio de 2008]. http://portal.acm.org/citation.cfm?id=948005.948022&coll=ACM&dl=ACM&CFID=39692116&CFTOKEN=62194334

[28]. Argarate, S. *Seguridad en las Transacciones online de Comercio Electrónico* (en líena). Tesis de Grado, México. [ref. de 4 de abril de 2008]. 127 p. http://www.monografias.com/trabajos-pdf/seguridad-e-comerce/seguridad-e-comerce.pdf

[29]. Will, Dormann & Jason, Rafail. *Securing your Web Browser* (en línea). CERT, febrero 14 de 2008 [ref. 20 de mayo de 2008]. http://www.cert.org/tech_tips/securing_browser

[30]. Nelte, M. & Elton, S. *Cookies: Weaving the Web into State* (en línea). 2004 [ref. 25 de mayo de 2008]. http://www.acm.org/crossroads/xrds7-1/cookies.html?searchterm=e-commerce+in+browser+web

[31]. Laboratorio Hispasec. *Troyano Bancario captura en video la pantalla del usuario* (en línea). 2006 [ref. 27 de mayo de 2008]. http://www.hispasec.com/laboratorio/troyano_bancario_captura_video.pdf

[32]. MacDoweell, M. *Browsing Safely: Understanding Active Content and Cookies* (en línea). National Cyber Alert System, Cyber Security Tip ST04-012.

Cert : 20 de junio de 2007 [ref. 12 de junio de 2008]. http://www.us-cert.gov/cas/tips/ST04-012.html

[33]. Creus Sole Antonio. *Fiabilidad y seguridad:su aplicación en procesos industrilaes* (en línea). Segunda Edición: 2005 [ref. 15 de junio de 2008]. 208 p. http://books.google.com.co/books?id=T6zqGALwitYC&pg=PA208&dq=cracker%2Bseguridad+informatica&sig=Bwn7mepTeR8BCt31ewP8v0F5Mhs#PPA13,M1

[34]. De la Cuesta, J. L. *Cuaderno del instituto vasco de criminología* (en línea), 2006 [ref. 17 de junio de 2008]. 181 p. http://www.ivac.ehu.es/p090-12133/eu/contenidos/boletin_revista/ivckei_eguzkilore_numero20/eu_numero20/adjuntos/13Inda_Polic.pdf

[35]. Asensio G. *Seguridad en Internet* (en línea). Universidad Politécnica de Madrid. Edición: Ilustrada. 2006 [ref. 20 de junio de 2008] 318 p. http://books.google.com.co/books?id=i6R5uhSeyOkC&pg=PA5&dq=seguridad+en+internet%2Bpharming&lr=&sig=dmu0XcvYgJLD5A2YYNj3tPIDv74#PPA5,M1

[36]. Asensio G. *Seguridad en Internet* (en línea). Universidad Politécnica de Madrid. Edición: Ilustrada. 2006 [ref. 20 de junio de 2008]. P 271. http://books.google.com.co/books?id=i6R5uhSeyOkC&pg=PA271&dq=que+es+firewall&lr=#PPA271,M1

[37]. W3C, Word Wide Web Consortion, *Guia Breve de Privacidad y P3P Oficina Española* (en línea). Enero de 2008 [ref. 30 de junio de 2008]. http://www.w3c.es/divulgacion/guiasbreves/PrivacidadP3P

[38]. VISA. *Seguridad de las compras* (en línea). [ref. de 1 de julio de 2008]. http://www.visalatam.com/s_personal/mundovirtual_descri.jsp

[39]. Network Working Group. *Site Security Handbook* (en línea). B. Fraser. SEI/CMU, septiembre de 1997 [ref. de 22 de mayo de 2008]. http://asg.web.cmu.edu/rfc/rfc2196.html

[40]. G. Alexander Alberto. *Diseño de un sistema de Gestión de Seguridad de Información: óptica ISO 27001:2005*. Bogotá: Alfaomega Colombiana S.A., 2007. 176 p. http://www.lalibreriadelau.com/catalog/product_info.php/products_id/12216?sid=0da40b805d260ffb614089e83f32c724

[41]. Ministerio de Administraciones Públicas. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. II – Catálogo de Elementos, NIPO 326 – 05 – 047 – X. Magerit versión 2 (en línea). Madrid: junio de 2006. 87 p. http://www.csi.map.es/csi/pdf/magerit_v2/catalogo_v11_final.pdf

[42]. Instituto Nacional de Tecnologías de la Comunicación INTECO. *Estudio sobre la Seguridad de la Información y eConfianza en los hogares españoles* (en línea). Abril de 2008 [ref. de 01 de julio de 2008]. p. 22.

http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_seguridad_hogares_oleada3

[43]. Instituto Nacional de Tecnologías de la Comunicación INTECO. *Estudio sobre Usuarios y Entidades Públicas y Privadas afectadas por la práctica fraudulenta conocida como Phishing* (en línea). 2007 [ref. de 5 de julio de 2008]. pp. 36, 64, 90, 104. http://www.inteco.es/search/Resultados_de_la_Busqueda/?allSearchField=Estudio+sobre+Usuarios+y+Entidades+P%C3%BAblicas+y+Privadas+afectadas+por+la+pr%C3%A1ctica+fraudulenta+conocida+como+Phishing

[44]. Instituto Nacional de Tecnologías de la Comunicación INTECO. *Estudio Confianza E-Commerce*. pp. 22, 29, 30, 46.

[45]. Instituto Nacional de Tecnologías de la Comunicación INTECO. *Ataques del día cero* (en línea). http://www.av-comparatives.org/seiten/ergebnisse_2008_05.php

[46]. Onestat.com. *Porcentaje de uso de distintos navegadores* (en línea). 2007 [ref. de 10 de agosto de 2008]. http://www.onestat.com/HTML/aboutus_pressbox53-firefox-mozilla-browser-market-share.html

[47]. Mozilla org. *Todas las extensiones para Firefox* (en línea). 2007 [ref. 20 de septiembre de 2008]. http://www.mozilla-hispano.org/tag/extensiones

[48]. Pressman R. *Ingeniería del Software un enfoque práctico (5ª Edición)*. Mc Graw Hill. España; 2002. 640 p.

[49]. Banco de Bogotá. *Políticas de privacidad* (en línea). https://www.bancodebogota.com/portal/page?_pageid=793,4324057&_dad=portal&_schema=PORTAL

[50]. Portal PayPal. *Centro de Seguridad* (en línea). https://www.paypal.com/es/cgi-bin/helpscr?cmd=_security-center-outside

[51]. Secretaría del Senado de la República. *Ley 527 de 1999* (en línea). Colombia: 1999. http://www.secretariasenado.gov.co/leyes/L0527_99.htm