C A P Í T U L O VII

CONCLUSIONES Y RECOMENDACIONES

7.1 Verificación de Hipótesis

La Hipótesis planteada en el Anteproyecto de Tesis fue:

El estudio de las formas y métodos de generación, manejo y administración de firmas digitales, permitirán conocer los distintos algoritmos de generación y dar criterios de evaluación sobre el uso de estas en el envió de información confidencial o no, sin ser alterada su estructura durante su camino. Así como dar alternativas de seguridad para los usuarios del Internet en el envío y recepción de información confidencial. Todo esto rigiéndose al marco legal que para cada situación geográfica se tenga.

Esta Hipótesis queda probada y demostrada de acuerdo a lo siguiente:

- Durante el desarrollo de la investigación se ha estudiado los distintos algoritmos de generación de firmas digitales, para la Infraestructura de Clave Pública, PKI.
- Se ha podido establecer con claridad la importancia de la Infraestructura de Clave Pública, como una tecnología necesaria en la actualidad para preservar la seguridad de la información que se transmite a través de cualquier medio que use una Red ya sea local o conectada al Internet
- A través de las firmas digitales se tiene la plena certeza de que el envío de información es confidencial y sólo el receptor de ésta información es quien puede descifrarla para su uso.
- Al estudiar los diferentes protocolos de seguridad para Internet, se ha podido establecer que SSL V3, es actualmente el protocolo

adoptado de manera general para la transmisión segura de información a través del Internet. Con lo que los usuarios están garantizados en el envío y recepción de su información sin repudio, alteración, o fraude y con autenticidad de quien lo envió.

- El proceso de envío y recepción de información mediante firmas digitales está respaldado y garantizado por las Autoridades de Certificación que son quienes dan Fé Pública de una persona que envía inflación a otra, es realmente quien dice ser, ya que está respaldada por la Firma Digital de la Entidad de Certificación.

7.2 Conclusiones

- A través de desarrollo de la presente investigación, como persona vinculada al uso y desarrollo de la tecnología, veo muy importante el estudio y uso de mecanismos de seguridad adecuados que permitan desarrollar alternativas de manejo y administración seguro de la información ya sea de una empresa, una institución educativa, pública, etc.
- En la actualidad en que nos encontramos en pleno y constante desarrollo de la tecnología, es necesario adoptar adecuadas políticas de seguridad para la transmisión de información a través de una red o del Internet. Las Firmas Digitales son el mejor mecanismo para hacerlo, no implica mayor costo ni dificultad en su obtención y uso.
- Una Firma Digital es un código numérico generado a través de un algoritmo criptográfico, que se lo puede adjuntar a cualquier mensaje o archivo a trasmitir a través del Internet con la que se garantiza la identidad de la persona que envía la información, siendo un medio probatorio legítimo para cualquier conflicto.

- Las Firmas Digitales desde el punto de vista Jurídico tienen la misma validez que una firma hecha con el puño y letra, por lo que no dan lugar a repudio, autenticidad y desconfianza por parte de quien las usa.
- Los Certificados Digitales son documentos públicos los cuales proporcionan la información necesaria acerca de su titular y de la Entidad de Certificación que da Fe Pública de que dicho certificado es válido para su uso, en cualquier transacción a través del Internet.
- Se ha podido determinar que existen diferentes maneras de implementar un sistema adecuado de seguridad, desde Seguridad de Directorio basado en Windows, Autenticación de usuarios a través de Login y Password, Biometría, Uso Criptografía de información y manejo de Firmas Digitales, el uso de cualquiera de éstos depende de las necesidades de cada organización y el campo de aplicación que se les dé.
- Las Autoridades de Certificación o El Estado, son las únicas organizaciones respaldadas por la Ley de Comercio Electrónico del Ecuador, que se encargan de gestionar, almacenar y dar Fe Pública de la validez de un certificado Digital. Así como de proveer servicios de Administración de Firmas y Certificados Digitales.
- De entre los algoritmos que existen para la generación llaves, certificados y firmas digitales se puede establecer que la mayoría de Países de nuestra América que tiene Legislación de Comercio Electrónico han adoptado a la Infraestructura de Clave Pública como sistema de seguridad adecuado, y los algoritmos RSA, ECC, SHA, MD5, como los algoritmos de facto para criptografía, firma digital y resúmenes.

7.3 Recomendaciones

- Es muy importante que se adopten estos mecanismos de seguridad a través de las Firmas Digitales por parte de empresas, organizaciones del sector público, educativo, comercial a fin de
- A los estudiantes se les recomienda prestar más atención a los aspectos de seguridad al momento de desarrollar sus proyectos y aplicaciones, una buena alternativa es el uso de firmas digitales y el encriptamiento de la información, usando certificados digitales, lo que les permitirá en la vida práctica desarrollarse con mayor capacidad.
- En la Universidad Técnica del Norte y en particular en la Escuela de Ingeniería en Sistemas Computacionales se debería apoyar y fomentar el estudio de este tipo de soluciones de seguridad, creando una materia de Criptografía y Seguridad o incluyendo en el pénsum de estudio de la materia de Ingeniería del Software este tema para que sea investigado por parte de los estudiantes.
- Se debería presentar un proyecto de prestación de servicios digitales y de criptografía por parte de la EISIC hacia las autoridades universitarias, para que la Universidad Técnica del Norte sea una Autoridad de Certificación reconocida en el Norte del País y permita a los estudiantes desarrollar sus capacidades intelectuales y optar por un medio de empleo y obtención de recursos.
- Para que los estudiantes puedan tener acceso a este tipo de tecnologías, se hace necesario dotar a la Biblioteca de la Facultad con el suficiente material didáctico para que los estudiantes tengan facilidades para poder usar e implementar en sus proyectos estudiantiles soluciones como estas y les permita desarrollar sus capacidades intelectuales.

Bibliografía

Libros

[LIB 01] Simson Garfinkel y Gene Spafford Seguridad y Comercio en el Web

[LIB 02] Lars Klander A prueba de Hackers

[LIB 03] Bull Casanova Firma Electrónica y Certificación Digital

[LIB 04] Anónimo Libro de Hackers

[LIB 05] Manuel Lucena López Criptografía y seguridad en Computadores

Direcciones de Internet

[WWW 001]
http://www.rsa.com/rsalabs/pubs/PKCS
Especificaciones de Criptosistemas de Clave Pública de RSA

[WWW 002]
http://www.htmlweb.net/seguridad/ssl/ssl_1.html
Seguridad SSL, Transacciones seguras en Internet

[WWW 003]
http://www.htmlweb.net/index.html Fundamentos de Criptografía

[WWW 004]
http://www.w3.org/TR/REC-html40 Firma Electrónica y Certificación Digital

[WWW 005]
http://www.pki-page.org/ Página oficial de la PKI (Public Key Infraestructure), especificaciones y Autoridades de Certificación mundial.

[WWW 006]
http://www.x9.org Organización de Estándares Internacionales

[WWW 007]
http://www.itu.int/itudoc/itu-t/rec/x/x500up/x509_27505.html
Sector de Estandarización de la

Unión Internacional de Telecomunicaciones.

[WWW 008]
http://www.iso.ch/cate/d17386.html Especificaciones de la Norma ISO/IEC 9594

[WWW 009]
http://www.iso.ch/cate/d17658.html Partes y especificaciones de la Norma ISO/IEC 9594

[WWW 010]
http://www.faqs.org/rfcs/rfc2527.html Especificaciones de Prácticas y Políticas de Certificación de Internet Standard X509.

[WWW 011]
http://www.mug.org.ar/Infraestructura/ArticInfraestructura/300.aspx
Autenticación LM, NTLM y Kerberos.

[WWW 012]
http://www.faqs.org/rfcs/ Índice de Request For Comment, Petición de Comentarios, RFC

[WWW 013]
http://www.pgp.com Sitio oficial del protocolo PGP

[WWW 014]
http://www.microsoft.com/latam/technet/articulos/windows2k/chapt-11/
Seguridad Distribuida para Windows 2000 (IPSec)

[WWW 015]
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html
Cryptographic Message Syntax Standard, Seguridad de RSA, PKCS #7

[WWW 016]
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html
Certification Request Syntax Standard, Seguridad de RSA, PKCS #10

[WWW 017]

http://www.pki-page.org/ Sitio Oficial de la Infraestructura de Clave Pública

[WWW 018]

http://www.is.escuelaing.edu.co/asignaturas/sypi

Página de la Escuela de Ingeniería de Colombia, Tecnologías Biométricas

[WWW 019]

www.emser.net/emser_en_castellano/Equipos_Portatiles.htm

Seguridad a través de Tarjetas Electrónicas

[WWW 020]

http://enciclopedia.us.es/index.php/ Implantación de una Infraestructura de Clave Pública

[WWW 021]

http://tejo.usal.es/~nines/d.alumnos/criptografia2/documentos/doc4_4.htm

Qué es X509V3

[WWW 022]

http://www.ietf.org/html.charters/pkix-charter.html

Estándares Internacionales PKIX, Public-Key Infrastructure (X_509).

[WWW 023]

http://www.upmadrid.edu.es/ Autoridades de Certificación y Confianza Digital

[WWW 024]

http://www.microsoft.com/technet/security/topics/secapps/authcode.mspx

Autenthicode de Microsoft

[WWW 025]

http://usuarios.lycos.es/sistemacomputacion/capitulodos3.htm

Técnicas de Seguridad del Comercio Electrónico

[WWW 026]

www.datasec.com.uy Criptografía Avanzada

[WWW 027]

http://www.htmlweb.net/seguridad/cripto/cripto_7.html

Manuales de Criptografía,
Algoritmos Simétricos

[WWW 028]
http://www.htmlweb.net/seguridad/cripto/cripto_7.html
Especificaciones de los
Algoritmos DES y Triple DES

[WWW 029]
http://enciclopedia.us.es/index.php/ Implantación de una Infraestructura de Clave Pública

[WWW 030]
http://www.htmlweb.net/seguridad/cripto/cripto_10.html
Especificaciones del Algoritmo RSA

[WWW 030]
http://www.htmlweb.net/seguridad/cripto/cripto_9.html
Especificaciones del Algoritmo
Diffie Hellman

[WWW 031]
http://www.htmlweb.net/seguridad/cripto/
Especificaciones sobre los
Algoritmos y funciones de Hashing.

[WWW 032]
http://www.iso.ch/cate/d17658.html Página de acceso a Estándares Internacionales sobre
Criptografía ISO - ANSI

[WWW 033]
http://www.x9.org/
http://www.itu.int/itudoc/itu-t/rec/x/x500up/ x509_27505. Html
Infraestructura X 509

[WWW 034]
http://www.rsa.com/rsalabs/pubs/PKCS
Página oficial de los estádares de
Criptografía PKCS de RSA.

[WWW 035]
http://www.iec.org Sitio oficial de la IEC

[WWW 036]
http://www.ietf.org Sitio oficial de la IETF
[WWW 037]
http://www.itu.int
http://www.itu.int/ITU-T/ Sitio oficial de la organización ITU internacional
[WWW 038]
http://www.ietf.org/html.charters/pkix-charter.html
Especificaciones sobre PKI, con referencia a X-509
[WWW 039]
http://www.ietf.org/html.charters/smime-charter.html
Organización de control sobre SMIME
[WWW 040]
ftp://ftp.isi.edu/in-notes/rfc2459.txt. Acceso al RFC 2459, sobre PKI, X509
[WWW 041]
ftp://ftp.isi.edu/in-notes/rfc2510.txt
Acceso al RFC 2510, sobre PKI X509 y protocolos de certificación
[WWW 042]
ftp://ftp.isi.edu/in-notes/rfc2560.txt
RFC 2560, sobre Protocolos de certificación On-Line.
[WWW 043]
ftp://ftp.isi.edu/in-notes/rfc2314.txt RFC 2314, sobre el Protocolo PKCS #10
[WWW 044]
ftp://ftp.isi.edu/in-notes/rfc2315.txt RFC 2315, sobre el Protocolo PKCS #7
[WWW 045]
ftp://ftp.isi.edu/in-notes/rfc2315.txt RFC 2315, sobre el Protocolo PKCS #7
[WWW 046]

ftp://ftp.isi.edu/in-notes/rfc2311.txt. Especificaciones de Seguridad sobre MIME, RFC 2311

[WWW 047]

ftp://ftp.isi.edu/in-notes/rfc2312.txt. Especificaciones de Seguridad sobre MIME, RFC 2312

[WWW 048]

ftp://ftp.isi.edu/in-notes/rfc2632.txt Especificaciones de Seguridad sobre MIME, RFC 2632

[WWW 049]

ftp://ftp.isi.edu/in-notes/rfc2633.txt Especificaciones de Seguridad sobre MIME, RFC 2633

[WWW 050]

ftp://ftp.isi.edu/in-notes/rfc2634.txt Especificaciones de Seguridad sobre MIME, RFC 2634

[WWW 051]

ftp://ftp.isi.edu/in-notes/rfc2630.txt Especificaciones de Seguridad sobre MIME, RFC 2630

[WWW 052]

ftp://ftp.isi.edu/in-notes/rfc2025.txt Mecanismos de Autenticación, RFC 2025

[WWW 053]

ftp://ftp.isi.edu/in-notes/rfc2743.txt. Mecanismos de Autenticación, RFC 2743

[WWW 054]

ftp://ftp.isi.edu/in-notes/RFC2246.TXT Mecanismos de Autenticación, RFC 2246

[WWW 055]

http://www.pki.gov.ar Autoridad de Certificación de la República de Argentina

[WWW 056]

http://www.internet.gouv.fr/francais/textesref/pagsi2/signelect /sommaire.htm Autoridad de Certificación de la República de Francia

[WWW 057]

http://www.aipa.it/attivita[2/standard[5/firmadigitale[2/index.asp
Autoridad de Certificación de la República de Argentina

[WWW 058]
http://www.aipa.it/attivita[2/standard[5/firmadigitale[2/index.asp
Autoridad de Certificación de la República de Argentina

[WWW 059]
http://www.monografias.com/trabajos17/delitos-electronicos/delitos-electronicos.shtml
Delitos informáticos

[WWW 060]
http://www.veraquinatana.com.ec
Análisis Jurídico del Comercio Electrónico en el Ecuador

[WWW 061]
http://www.corpece.org.ec
Corporación Ecuatoriana de Comercio Electrónico

[WWW 062]
http://www.corpece.org.ec/documentos/articulos/nacionales/electronico-marklaw.htm
Análisis de la Ley de Comercio Electrónico del Ecuador, Marklaw

[WWW 063]
http://www.revistasdederecho.com/firmadigital
Recopilación de las leyes de Comercio electrónico en el Mundo

[WWW 064]
http://www.alfa-redi.org/revista/data/20-9.asp
Análisis de la Ley de Comercio Electrónico y Firmas Digitales del Ecuador, José Luis Varsallo

[WWW 065]
www.uncitral.org
Página oficial de la Ley Modelo UNCITRAL