

**FUNDAMENTOS PARA EL DESARROLLO DE UN
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN**

JERSON VIVEROS AGUIRRE

Anteproyecto del trabajo de grado presentado como
requisito para optar al título de Ingeniero Electrónico.

Director:

Profesor: OSCAR POLANCO

**UNIVERSIDAD DEL VALLE
ESCUELA DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA
INGENIERÍA ELECTRÓNICA SANTIAGO DE
CALI**

2005

Profesor Ing. OSCAR POLANCO
DIRECTOR DEL PROYECTO

Profesor Ing. FABIO GUERRERO, MSc.
COORDINADOR DEL ÁREA DE
TELECOMUNICACIONES

Profesor Ing. CARLOS PINEDO
DIRECTOR DEL PLAN DE ESTUDIOS
INGENIERÍA ELECTRÓNICA

TABLA DE CONTENIDO

1. INTRODUCCIÓN	2
2. ANTECEDENTES.....	3
3. FORMULACIÓN DEL PROBLEMA.....	5
4. JUSTIFICACIÓN.....	6
5. OBJETIVOS	7
5.1. OBJETIVO GENERAL	7
5.2. OBJETIVOS ESPECÍFICOS.....	7
6. MARCO TEÓRICO	8
7. ESTADO DEL ARTE	9
8. RESULTADOS ESPERADOS.....	10
9. METODOLOGÍA	11
10. CRONOGRAMA DE ACTIVIDADES.....	12
11. PRESUPUESTO.....	13
12. GLOSARIO	14
13. REFERENCIAS.....	15

1. INTRODUCCIÓN

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. La necesidad imperante del flujo de información y el traslado de recursos de un sitio a otro hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad de la infraestructura de comunicación y toda la información que contienen sus nodos. Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Las amenazas que se pueden presentar provienen tanto de agentes externos como de agentes internos, por eso es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques a los que se expone defina una estrategia de seguridad fundamentada en políticas que estén respaldadas por todos los miembros de la organización.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de la empresa y dejarla expuesta a la quiebra.

En este trabajo se discute el tema de seguridad de la información, se destacan mediante ejemplos las características más importantes de los mecanismos que actualmente utilizan los atacantes de la red, se identifican los fundamentos para el desarrollo de un sistema de gestión de seguridad de la información y para la creación de una estrategia de seguridad basada en políticas, se desarrolla un módulo de software para la redacción y almacenamiento de políticas de seguridad de la información y se analizan algunas de las herramientas de gestión de seguridad existentes.

2. ANTECEDENTES

El número de atacantes de las redes y de los sistemas en las organizaciones es cada vez mayor y las técnicas empleadas mejoran constantemente. Existen muchos grupos interesados en el tema de seguridad, muchas personas participan activamente en el desarrollo de nuevas técnicas que permitan aprovechar los huecos de seguridad.

Los trabajos encontrados en la Universidad sobre el tema de seguridad son los siguientes:

“Manual de detección de vulnerabilidades de sistemas operativos UNIX¹ en redes TCP/IP²” [4], en éste se destacan las vulnerabilidades mas comunes y se elabora un manual de seguridad para Sistemas UNIX.

“Estudio de seguridad en computadoras con sistemas operativos UNIX conectados a una red TCP/IP” [5], En este trabajo se tocan de forma general los temas relacionados con la seguridad de la información, se definen algunos conceptos básicos y se habla de algunas herramientas para ataque y protección de sistemas UNIX.

“Seguridad en transacciones con base de datos a través de una página web” [6], en este trabajo se destacan algunos conceptos básicos de seguridad de la información.

“Implementación de un algoritmo para mejorar la seguridad de un sitio web utilizando una técnica de criptografía en una arquitectura de interfaz CGI³” [7], en este trabajo se definen los conceptos de criptografía, se estudian algunos algoritmos de criptografía y se implementa un algoritmo usando una técnica de criptografía sobre una interfaz CGI.

La principal diferencia del trabajo a realizar con respecto a los trabajos realizados en la universidad sobre el tema radica en el énfasis que se hace sobre los fundamentos

¹ Sistema Operativo Multiusuario y Multitarea.

² Transfer Control Protocol/ Internet Protocol

³ Common Gateway Interface

del desarrollo de un sistema de gestión de seguridad de la información basado en las normas internacionales como la británica BS 7799 y la ISO 17799, además del desarrollo de un módulo de software que sirva para la redacción y el almacenamiento de políticas de seguridad de la información.

Los trabajos encontrados en otras partes sobre el tema son:

Manual de Seguridad en Redes [3], en este trabajo se exponen las consideraciones que se deben tener en cuenta para el establecimiento de una estrategia de seguridad.

Código de práctica para la administración de la seguridad de la información, IRAM⁴-ISO IEC 17799 [2], este trabajo es una traducción al español de la norma ISO 17799 que se encuentra vigente en la actualidad y donde se exponen las mejores prácticas de seguridad de la información.

El informe encargado por McAfee del 5 de julio de 2005 [8] establece un panorama claro de la crecientes amenazas y delitos que se cometen mediante Internet, analiza las amenazas futuras que esta actividad puede significar para las computadoras domésticas, las redes computacionales de las organizaciones gubernamentales y los sistemas computacionales del sector empresarial.

Los aspectos más destacados del informe indican:

- “El FBI estima que el crimen cibernético costó aproximadamente US\$400 mil millones en el año 2004.”
- “En una investigación denominada “Operation Firewall” las autoridades estadounidenses y canadienses anunciaron el arresto de 28 personas de seis países, que estaban involucradas en una red mundial de crimen cibernético organizado.”
- “Según estimaciones, probablemente sólo el 5% de los criminales cibernéticos son capturados y procesados.”

⁴ Instituto Argentino de Normalización

En el congreso Internacional de seguridad informática H@cker Halted 2005⁵ [9] organizado por el Consejo Internacional de Consultores de Comercio Electrónico (EC-Council) se destaca lo siguiente:

- “Cada PC conectada al Internet tiene por lo menos tres intentos de ataques diarios. La mayoría de los usuarios desconocen esto.”
- “Al interior de las empresas la mejor forma de combatir este delito es mediante la concienciación de los usuarios, la actualización de sistemas y equipos, así como a través de la instauración de políticas internas y el otorgamiento de prioridades.”
- “Advierten además que la industria del software de seguridad se encuentra en un periodo de transición acelerada ante la magnitud de pérdidas y fraudes cometidos.”

3. FORMULACIÓN DEL PROBLEMA

La complejidad en el manejo de la seguridad de la información hace que sea necesario desarrollar un sistema de gestión de seguridad informática que sirva para administrar la seguridad.

Como parte de la implementación de un sistema de gestión de seguridad de la información, las organizaciones crean políticas que deben estar asociadas a la protección de los activos informáticos. Se requieren herramientas de software que sirvan para redactar, clasificar y almacenar las políticas de manera que puedan ser accedidas en cualquier momento por las personas responsables.

El área de telecomunicaciones de la Universidad del Valle no se ha apropiado del conocimiento suficiente, ni cuenta con herramientas de software que sirvan para trabajar el tema de seguridad de la información para redes de comunicación con base en un sistema de gestión.

⁵ Hacker Halted es un congreso internacional realizado anualmente donde se trabajan problemas de seguridad de la información.

4. JUSTIFICACIÓN

Los antecedentes muestran la tendencia a que el tema de seguridad tome cada vez mayor importancia al interior de las organizaciones, existe por lo tanto una gran oportunidad de negocio para las personas capacitadas en el tema en la medida en que sea creciente el número de organizaciones que necesiten asegurar sus sistemas, bien sea porque quieran certificarse para garantizar que sus sistemas son seguros o porque de alguna forma han sufrido ataques y pretenden desarrollar una estrategia de seguridad basándose en las mejores prácticas de aseguramiento de la información expuestas en las normas internacionales.

Considerando que el área de Telecomunicaciones de la Escuela de Ingeniería Eléctrica y Electrónica no cuenta con información clara sobre cómo crear una estrategia de seguridad, cómo definir las políticas de seguridad, cuáles son los recursos que se deben proteger, qué procedimientos debe tener la empresa para cumplir los objetivos de seguridad, qué personas están involucradas en el establecimiento de las políticas y quiénes deben velar por hacerlas cumplir; y que no cuenta con herramientas de software que sirvan de soporte para capacitar a los estudiantes en el tema de seguridad, se hace importante la apropiación de conocimiento en el tema y el desarrollo de una herramienta de software. El presente anteproyecto está articulado con tres trabajos adicionales que se enfocarán en tópicos específicos del tema de seguridad donde se trabajaran los problemas de autenticación, seguridad perimetral y seguridad sobre en redes virtuales privadas.

5. OBJETIVOS

5.1. Objetivo General

Desarrollar un estudio, basado en la norma BS7799-2, para la creación de una estrategia de seguridad de la información en redes y sistemas informáticos.

5.2. Objetivos Específicos

- ◆ Desarrollar un módulo de software para la redacción y almacenamiento de políticas de seguridad de la información, basados en el primer dominio de la norma ISO 17799.
- ◆ Aplicar los controles de la norma ISO 17799 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un sistema de gestión de seguridad de la información.
- ◆ Elaborar una guía básica para el desarrollo de una estrategia de seguridad informática, basado en las normas internacionales que recogen las mejores prácticas de seguridad.
- ◆ Identificar y probar 6 de los mecanismos usados comúnmente para producir ataques de seguridad, considerando las vulnerabilidades de los sistemas.
- ◆ Evaluar 2 herramientas de software existentes para gestión de seguridad informática por medio de sus versiones de demostración.

6. MARCO TEÓRICO

Las políticas y los procedimientos de seguridad informática surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información que favorecen el desarrollo y el buen funcionamiento de la organización. Deben considerarse como reglas a cumplir que surgen para evitar problemas y que se establecen para dar soporte a los mecanismos de seguridad implementados en los sistemas y en las redes de comunicación.

Un plan de seguridad en una organización debe estar soportado por políticas y procedimientos que definan porque proteger un recurso, que quiere hacer la organización para protegerlo y como debe procederse para poder lograrlo.

Una de los aspectos más importantes que se debe considerar, en el desarrollo de políticas de seguridad, es poder determinar qué es lo que se quiere proteger y de qué se quiere proteger. Para lograr esto es importante tener conocimiento de las vulnerabilidades y formas de ataque de los sistemas con que cuenta la organización.

Los ataques internos los pueden realizar personas con buen conocimiento de técnicas para acceder a cuentas a las que no están autorizados o pueden surgir como accidentes que se presentan por el mal uso de los recursos. Los ataques externos provienen de personas experimentadas en acceder a los sistemas a través de las diferentes modalidades en que las compañías se conectan al Internet. En general estas personas poseen buenos conocimientos sobre Software, Hardware, programación, Lenguaje Ensamblador, Sistemas Operativos, TCP/IP, protocolos de seguridad, etc. Algunos de estos son expertos en Ingeniería social, es decir que son capaces de engañar a los usuarios autorizados para que les terminen dando acceso a los sistemas.

Algunas de las herramientas usadas por los atacantes se describen a continuación:

Sniffers

Programas que se dejan ocultos en los servidores para que espíen las conexiones y se puedan detectar los logins, passwords y demás información.

Programas de ocultamiento (zappers)

Son unos programas que borran las huellas de los ataques que se han hecho en los sistemas.

Crackeadores:

Herramientas que permiten averiguar las claves de un sistema aunque estén encriptadas.

Una de las herramientas más utilizadas en la prevención de ataques externos por parte de los intrusos de Internet (Hackers) es el **Firewall** que ofrece seguridad de protección contra intrusos determinando que servicios de la red pueden ser accedidos y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no autorizados y en caso de un ataque genera alarmas de seguridad. La implementación de Firewalls debe soportarse dentro del marco de un sistema de gestión de seguridad de la información y debe ser respaldado por políticas de seguridad que definan las normas de acceso a la red.

Los Firewalls son una puerta de acceso entre el Internet y la red Interna, también pueden ser puertas de acceso entre diferentes subdivisiones de una red. Esta aplicación determina que paquete puede pasar y cual no. Puede operar a nivel de aplicación o sobre las capas de red o transporte.

7. ESTADO DEL ARTE

Las organizaciones que requieren implementar una estrategia de seguridad para proteger su información bajo los estándares internacionales, deben desarrollar e implantar un SGSI (sistema de gestión de seguridad de la información). Este proceso de administración y certificación de seguridad se debe hacer según las normas ISO 17799/ BS-7799-2.

El estándar británico BS 7799-2 determina los requisitos para establecer y administrar un sistema de gestión de seguridad de la información (SGSI), Su primera versión sale en el año de 1995 como recomendaciones para seguridad basadas en las mejores prácticas, se hacen modificaciones a esta norma en los años 1998, 1999, 2001 y

finalmente es actualizada en el año 2002 y corregida para convertirse en un estándar certificable aceptado actualmente por el ICONTEC en Colombia, aunque a la fecha no se conoce ninguna empresa certificada bajo este estándar en el país.

La norma ISO 17799:2000 contiene las recomendaciones para el aseguramiento de la información que se basan en las mejores prácticas de seguridad, esta norma es una evolución del estándar británico BS 7799 en su primera versión, no es certificable pero debe ser adoptado por las organizaciones que quieran obtener la certificación BS 7799-2:2002; cubre aspectos como el manejo de equipos, la administración de políticas, los recursos humanos y los aspectos legales entre otros. Esta norma se basa en 10 Dominios de control:

- ◆ Política de seguridad
- ◆ Organización de la seguridad
- ◆ Clasificación y control de recursos
- ◆ La seguridad del personal
- ◆ La seguridad física y ambiental.
- ◆ Administración de comunicaciones y operaciones
- ◆ Control de acceso
- ◆ Desarrollo y mantenimiento de sistemas
- ◆ Plan de continuidad del negocio
- ◆ Cumplimiento de normatividad legal

Cada dominio busca cumplir con unos objetivos que suman 56 en total. Para cumplir los objetivos se deben evaluar 127 controles que son las recomendaciones de la norma, las organizaciones deciden si adoptar o no el control dependiendo del nivel de seguridad que desean para sus activos informáticos.

8. RESULTADOS ESPERADOS

Al final del proyecto se espera tener un módulo de software que permita realizar la redacción, el almacenamiento y la administración de las políticas de seguridad de la información. Se espera tener los fundamentos básicos que permitan el desarrollo de un sistema de gestión de seguridad de la información y se espera tener los resultados

de evaluación de 6 herramientas utilizadas para la realización de ataques en sistemas de información.

9. METODOLOGÍA

La realización del trabajo de grado depende del desarrollo de varias etapas en la adquisición de conocimiento, en la realización de pruebas y en el desarrollo del módulo de software.

ETAPA 1

Apropiación del conocimiento en sistemas de gestión de seguridad de la información para sistemas y redes de comunicación. De esta forma se espera crear un referente teórico que sirva de base para el desarrollo del trabajo de grado y del documento a presentar

Apropiación del conocimiento en los mecanismos existentes para la detección de intrusos.

ETAPA 2

Simulación de los 6 tipos de ataques más frecuentes que pongan en riesgo la seguridad de un sistema o una red a fin de tener mejores fundamentos en la creación de políticas y procedimientos.

ETAPA 3

Aplicación de los controles de la norma ISO 17799 que permitan administrar un sistema de detección de intrusos dentro de un sistema de gestión de seguridad de la información.

ETAPA 4

Evaluación de 2 herramientas de software para sistemas gestión de seguridad informática existentes en el mercado actualmente.

ETAPA 5

Desarrollo del módulo de software para la redacción y almacenamiento persistente de políticas de seguridad de la información.

ETAPA 6

Elaboración del documento que identifica los fundamentos básicos para el desarrollo de una estrategia de seguridad de la información, basado en las normas internacionales.

10. CRONOGRAMA DE ACTIVIDADES

Como se mencionó en la metodología, el desarrollo del trabajo de grado consta de 6 etapas. El cronograma de actividades para la ejecución del proyecto se presenta en el cuadro 1.

ETAPA	NOV. 2005	DIC. 2005	ENE. 2006	FEB. 2006	MAR. 2006	ABR. 2006	MAY. 2006	JUN. 2006	JUL. 2006	AGO. 2006	SEP. 2006
1	■	■									
2			■	■							
3					■						
4			■	■	■	■					
5							■	■	■	■	■
6										■	■

TABLA 1. Cronograma de actividades.

11. PRESUPUESTO

El trabajo de grado se financiará con recursos propios y del área de telecomunicaciones de la Universidad del Valle. En la tabla se presenta una relación de costos detallada.

Recurso	Función	Tiempo dedicación	Valor Hora	Total
Ing. Oscar Polanco	Director	40	\$ 25.000	\$ 1.000.000
Jerson Viveros	Tesista	960	\$ 15.000	\$ 14.400.000
Total				\$ 15.400.000

Tabla 1: Recursos Humanos

Recursos	Fuente	Valor
Computador personal	Propios	\$ 600.000
Puesto de trabajo con punto de red	Universidad	\$ 2.000.000
Equipos de red (Routers y Switch)	Universidad	\$ 1.000.000
Norma BS7799-2/ISO 17799	Propios	\$ 80.000
Libros	Propios	\$ 100.000
Papelería	Propios	\$ 100.000
Total		\$ 3.880.000

Tabla 2: Recursos Físicos

12. GLOSARIO

UNIX: desde el punto de vista técnico, UNIX se refiere a una familia de sistemas operativos que comparten unos criterios de diseño e interoperabilidad en común. Esta familia incluye más de 100 sistemas operativos desarrollados a lo largo de 20 años. No obstante, es importante señalar que esta definición no implica necesariamente que dichos sistemas operativos compartan código o cualquier propiedad intelectual [10].

Transfer Control Protocol/ Internet Protocol: El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa [11].

Common Gateway Interface: Un CGI (Common Gateway Interface) es un programa que se ejecuta en tiempo real en un Web Server en respuesta a una solicitud de un Browser. Cuando esto sucede el Web Server ejecuta un proceso hijo que recibirá los datos que envía el usuario (en caso de que los haya), pone a disposición del mismo algunos datos en forma de variables de ambiente y captura la salida del programa para enviarlo como respuesta al Browser [12].

13. REFERENCIAS

- [1] Network Working Group, "Site Security Handbook" , Request for Comments 2196, Septiembre 1997.
- [2] Instituto Argentino de Normalización, "Código de práctica para la administración de la seguridad de la información", IRAM-ISO IEC 17799, Buenos Aires, febrero 2002.
- [3] Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina, Manual de Seguridad en Redes.
- [4] Jesús Herney Cifuentes, César Augusto Narváez, Manual de detección de vulnerabilidades de sistemas operativos UNIX en redes TCP/IP, Universidad del Valle 2004.
- [5] Gustavo Adolfo Barreto, Estudio de seguridad en computadoras con sistemas operativos UNIX conectados a una red TCP/IP, Universidad del Valle 2001.
- [6] Liliana Rojas, Humberto Campiño, Seguridad en transacciones con base de datos a través de una página web, Universidad del Valle 2002.
- [7] Oscar Javier Dorado, Implementación de un algoritmo para mejorar la seguridad de un sitio web utilizando una técnica de criptografía en una arquitectura de interfaz CGI, Universidad del Valle 2001.
- [8] Charles Davis, Eric Lakin, "Hasta las Pymes son Hacheadas", Exposición en el Congreso Internacional en Seguridad TI Informática H@cker Halted 2005.
- [9] McAfee, "Estudio de criminología virtual McAfee", Julio 2005, disponible en: http://www.mcafeesecurity.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf
- [10] GNU Free Documentation License, "UNIX", disponible en : <http://es.wikipedia.org/wiki/Unix>
- [11] GNU Free Documentation License, " familia de protocolos de Internet", <http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml>
- [12] Monografías online, "CGI Master", disponible en: <http://www.ok.cl/cgi/chap0/>.