INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS GUADALAJARA

PROGRAMA DE GRADUADOS EN INGENIERIA Y TECNOLOGIA

DISEÑO DE UN METODO DE PREVENCION Y DETECCION DE VIRUS GUSANO PARA MITIGAR EL IMPACTO ECONÓMICO Y MANTENER LA PRODUCTIVIDAD AL SER IMPLEMENTADO EN LAS UNIVERSIDADES DE MÉXICO

TESIS

POR

RAMIRO ALEJANDRO BERMUDEZ URIBE

Guadalajara Jalisco diciembre de 2005

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS
SUPERIORES DE MONTERREY

CAMPUS GUADALAJARA

PROGRAMA DE GRADUADOS EN INGENIERÍA Y TECNOLOGÍA

TECNOLÓGICO
DE MONTERREY®

DISEÑO DE UN MÉTODO DE PREVENCIÓN Y DETECCION DE VIRUS GUSANO PARA MITIGAR EL IMPACTO ECONÓMICO Y MANTENER LA PRODUCTIVIDAD AL SER IMPLEMENTADO EN LAS UNIVERSIDADES DE MÉXICO

TESIS

POR:

RAMIRO ALEJANDRO BERMÚDEZ URIBE

Guadalajara Jalisco diciembre de 2005

DISEÑO DE UN MÉTODO DE PREVENCIÓN Y DETECCIÓN DE VIRUS GUSANO PARA MITIGAR EL IMPACTO ECONÓMICO Y MANTENER LA PRODUCTIVIDAD AL SER IMPLEMENTADO EN LAS UNIVERSIDADES DE MÉXICO

POR:

RAMIRO ALEJANDRO BERMÚDEZ URIBE

TESIS

Presentada al Programa de Graduados en Ingeniería y Tecnología.

Este trabajo es requisito parcial para obtener el grado de Maestro en Administración de las Tecnologías de Información

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

diciembre 2005

Dedicatoria

A Cristy... por su apoyo y ayuda. Gracias por la paciencia y por estar conmigo en todos estos años del desarrollo de la maestría.

Agradecimientos

A Dios por su ayuda en toda mi vida.

A mi familia.

A mi comité de tesis por el apoyo brindado para la realización de esta tesis.

A todos los que apoyaron a la contribución de este estudio.

Gracias.

Resumen

El valor agregado de los sistemas de información a la productividad de las empresas, en los últimos años, ha propiciado su competitividad y distinción. Las universidades, como empresas que vende educación de calidad, han tomado también sustento en las tecnologías de información para renovar su estrategia educativa y cubrir las exigencias de un mercado más demandante y con movilidad.

Ahora bien, los sistemas de información son vulnerables a lo que se le conoce como amenazas informáticas. Éstas, impactan en la productividad y la economía de toda empresa; así como en costos indirectos; como lo son la imagen y los distintivos.

Existen consultoras y métodos para encarar sistemáticamente las amenazas de seguridad informática; pero existe un tipo de empresa en específico que no ha sido concebida, desde sus orígenes, directamente para trabajar con seguridad informática; estas empresas son las universidades.

El diseñó de un método para encarar a los virus gusano (worms), como una amenaza de seguridad importante, será tratado en este estudio para evaluar el impacto económico y la productividad de las universidades de México al ser implementado dicho método.

Índice

Lista de figuras

Lista de tablas

Capítulo 1

Investigación

Existen varias amenazas en las comunicaciones empresariales. Una de ellas y la cual genera más impactos; es la propagación de los virus gusano (worms). Se pretende en este capítulo, identificar, situar y conocer el problema que se origina en las industrias, empresas y universidades así como las áreas de oportunidad a atender que en el estudio se centrarán a la productividad y las pérdidas económicas. Después se presentará el acotamiento del tema de la tesis, objetivo, motivación, distribución del estudio y contribución esperada de la tesis.

1. 1 Situación de la problemática

Haciendo un breve antecedente histórico, encontramos que antes de la segunda guerra mundial la economía se centraba en generación de bienes físicos (activos tangibles) y al término de la guerra, el producto interno bruto (PIB) de varios países se centra en la generación de servicios (activos intangibles). Un ejemplo de estos países es Canadá, que ofrece más servicios como productos de exportación que productos materiales (Carrillo, 2002).

Un gran apoyo a la generación de estos servicios o el mismo sustento de ellos, en su mayor parte, han sido las tecnologías de información. Estas tecnologías además, apoyan a las empresas, industrias y universidades para hacerlas mas eficientes, generarles ventajas competitivas y tener mas beneficios.

Es entonces, que en la gran mayoría de nuestro trabajo diario tenemos contacto con alguna tecnología de información y que al no tener presente dicha tecnología de información; mina nuestra productividad y puede acarrear pérdidas económicas a nuestra organización (Gallivan, 2000)

Ahora bien, con el creciente uso del Internet, las organizaciones no sólo se comunican con las demás organizaciones, sino que se ven expuestas a variables o amenazas que pueden comprometer sus tecnologías de información.

1.2 Conocimiento del problema

Se define como sistema en general, al conjunto de dos o más elementos interrelacionados, de cualquier especie, que buscan un objetivo en común. Existen sistemas cerrados que no tienen relaciones con su medio y sistemas abiertos que intercambian información con su medio. Sin embargo, no encontramos un sistema totalmente cerrado y esto es debido a una complejidad dinámica y de elementos de retroalimentación, modelos mentales reales, estrategias, estructuras y sobre todo decisiones en un tiempo determinado (Sterman, 2003 pag 19,20).

Centrándonos en materia de los sistemas de información. Los sistemas de información que no tienen contacto con el exterior de la empresa en intercambio de datos, se pueden ver interferidos en sus operaciones por variables de la misma compañía. Los sistemas de información que interactúan con el exterior de la compañía como en una red de datos wan o de Internet pueden tener un gran número de variables o amenazas que interfieran en su trabajo normal.

Las amenazas e incidentes provocados por éstas, han ido en aumento en los últimos años. La universidad Carnegie Mellon con su equipo de respuesta para emergencias informáticas (CERT) en la dirección electrónica http://www.cert.org/stats/ muestra el significativo aumento a partir del año de 1999 representado en la figura 1.1

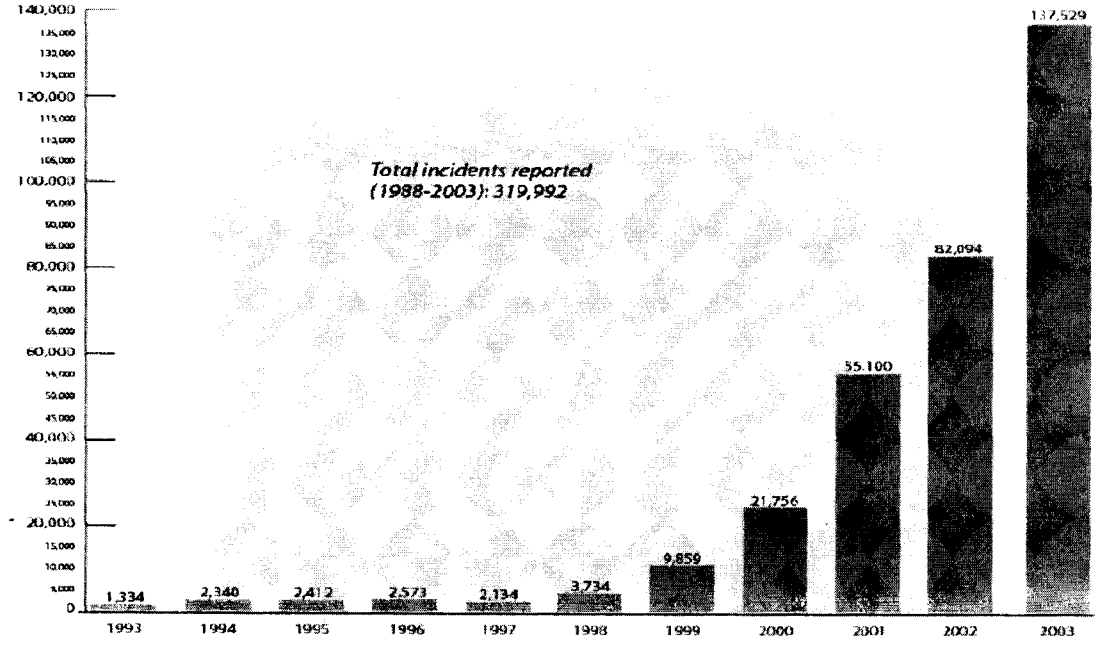


Figura 1.1 Contabilización de incidentes de seguridad por parte del CERT. Gráfico tomado del white paper de Nicholas John Lippis de Lippis Consulting.

A estos incidentes, los denominaremos violaciones de la seguridad de información que afecta a tres principios de la información: la integridad, la confidencialidad y la disponibilidad (Academia Latinoamericana de Seguridad Informática, 2005).

De acuerdo con la Academia Latinoamericana de Seguridad Informática la cual es un esfuerzo conjunto de las empresas E-modulo Security y Microsoft con el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) en su sistema de educación virtual, definen los tres principios de la información como:

- **Integridad:** al proceso de tener la información correcta. Nos permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra. Se espera *evitar Alteraciones del contenido y Alteraciones en los elementos que soportan la información.*

- **Confidencialidad:** al proceso que permite transferir información de un emisor a al adecuado receptor sin que un tercero pueda obtener la información enviada. Se dice que la información posee un grado de confidencialidad que se deberá preservar para que personas sin autorización no la conozcan. *Pérdida de confidencialidad significa pérdida de secreto.*

- **Disponibilidad:** presentar la información en el momento adecuado para su utilización. La disponibilidad de la información y de toda la estructura física y tecnológica es permitir el acceso, tránsito y almacenamiento adecuado en forma segura que permita ser confidencial e íntegra.

Otro nombre común para las amenazas de los sistemas de información (threats en inglés) es amenazas informáticas. Existen un gran número de amenazas de informáticas como lo son:

- Malware (programas maliciosos).
- Hackers (personas maliciosas).
- DOS (denegación de servicio).
- Spam (correos no deseados).
- Ataques sofisticados.
- Robos de identidad.
- Explotación de vulnerabilidades.
- Phishing (fraudes en información)

1.3 Amenazas informáticas en los sistemas de información de las universidades

Ahora bien, las empresas no son las únicas expuestas a amenazas a sus sistemas de información. Como tal, una universidad es una institución que su negocio principal es la educación y por tal motivo, también esta expuesta a amenazas informáticas.

Consultando un artículo de seguridad de Symantec, quien es una firma importante de antivirus, comenta que a diferencia de las redes corporativas y otras redes comerciales, que son más cerradas y segmentadas con énfasis en la protección de los recursos valiosos de la información, las redes de la universidades están diseñadas para funcionar como proveedores del servicio de Internet, facilitar el acceso a los usuarios y facilitar el flujo de la información.

Históricamente, el cuerpo docente, los investigadores y estudiantes de las universidades han esperado, y en algunos casos solicitado, acceso gratuito y abierto a los sistemas informáticos universitarios. A la luz de las recientes brechas de seguridad divulgadas, que se mencionaron anteriormente, y de las expectativas de más amenazas a la seguridad en el futuro, no puede continuar este acceso abierto e ilimitado. Los administradores de tecnología de información (TI) con frecuencia caminan en la cuerda floja cuando se trata de restringir las redes universitarias sin afectar la naturaleza abierta de las comunicaciones a la que están acostumbrados los estudiantes y el cuerpo docente.

El artículo fue publicado el 28 de abril del 2004 titulado "Las universidades abordan el problema del robo de identidad".

1.4 Ubicación de las amenazas de los programas maliciosos (malware) a los sistemas de información

La estructura que agrupa los comportamientos generales de un virus; se le conoce como malware. El malware es un código o programa malicioso que comprometen los sistemas de información (Trend Micro, firma de antivirus).

En la figura 1.2 nos muestra las diferentes formas de códigos maliciosos (malware) que existen y que comprometen a los sistemas de información:

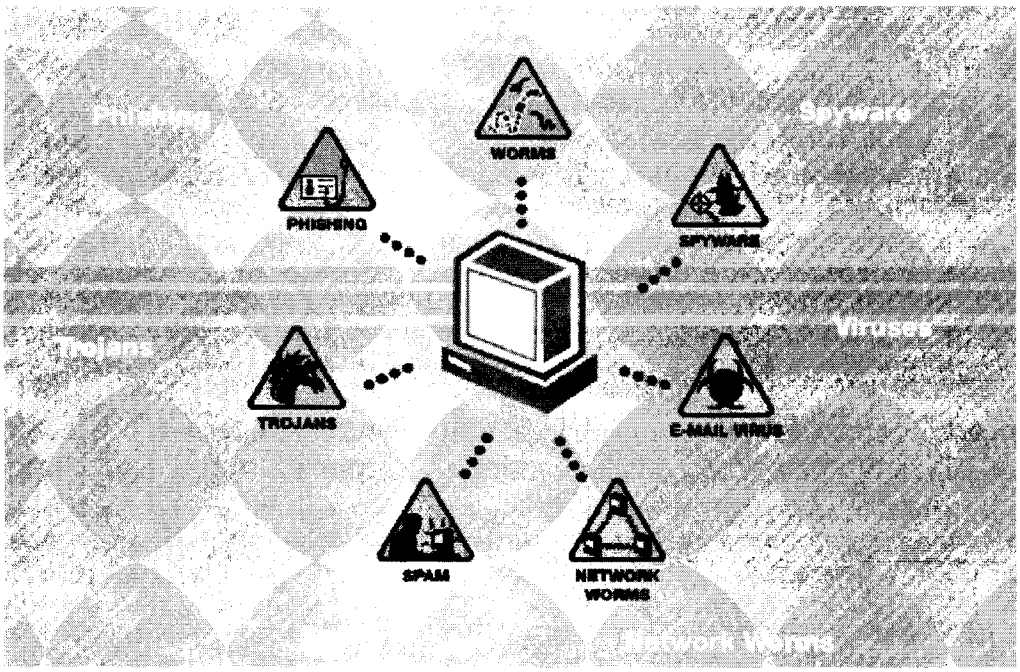


Figura 1.2 Formas en la que se presentan los códigos maliciosos (malware).

La revista tecnología empresarial comenta que en cuanto a los códigos maliciosos, se observó un aumento de 300% de las vulnerabilidades para aplicaciones Windows de 32 bits en el 2004. Symantec documentó 4,496 nuevos virus y gusanos del sistema Windows en este periodo.

Para el estudio es importante definir los diferentes integrantes de los códigos maliciosos (malware) para posteriormente acotar a uno donde el estudio revela impacta mas a los sistemas de información y la productividad de los usuarios de estas tecnologías..

Las definiciones usadas son:

Virus: Es un programa de computadora que puede infectar otros programas. El primer virus que atacó a una máquina IBM 360 (y reconocido como tal), fue llamado Creeper, creado en 1972 por Robert Thomas Morris. Este programa emitía periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora). Tomado de la enciclopedia wikipedia.

Fred Cohen en su tesis doctoral en 1984 advertía que los virus serían un problema muy importante en el futuro.
e-mail virus: Es un programa de computadora que puede infectar otros programas y que se obtiene por abrir archivos adjuntos en un correo electrónico (mail). Generalmente son molestos pero también pueden ser destructivos; borrar datos, archivos o formatear máquinas. Tomado de Trend Micro.

Troyanos: Virus que toman la misma estrategia que la famosa historia griega. Ofrecen un regalo o programa "llamativo", como por ejemplo programas para bajar archivos con terminación mp3 como el Kazza, para después en un tiempo de bajar la guardia se introducen en el sistema, Tomado de Trend Micro.

Spam: Correo electrónico (mails) recibidos de personas desconocidas o conocidas con material de contenido explícito como sexo, invitaciones, ofertas o juegos. Contiene generalmente archivos adjuntos con virus o virus gusanos (worms). El 50% aproximadamente del tráfico mundial es spam. Tomado de Trend Micro.

Spyware: Programas que pueden ser instalados conciente o inconscientemente de una fuente de spam, virus, troyanos o programas de dudosa procedencia. Recolectan información sensible como nombres, claves, números de tarjetas crédito, números confidenciales, etc. para ser mandados a terceros. Tomado de Trend Micro.

Phishing: Estrategia para recolectar información directamente de la victima. Se recibe por spam, puede ser acompañada de cualquier amenaza anterior. Presenta una trampa para proporcionar información sensible directamente a páginas electrónicas (web) idénticas en apariencia al banco que usa la victima. Decepción en las víctimas y pérdidas económicas. Tomado de Trend Micro.

Virus gusanos (worms): En informática, un gusano es un virus o programa que no altera los archivos sino que reside en la memoria y se replica a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias

del mismo son excesivamente lentas o simplemente no pueden ejecutarse. Tomado de Trend Micro.

Virus gusanos (worms) en red: Explotan vulnerabilidades de los sistemas operativos por ejemplo Windows. El contagio es por sólo estar en la red y se replican de máquina en máquina a una impresionante velocidad. Se ocultan muy bien; por lo que los antivirus no lo detectan con facilidad. Generan un desmedido tráfico en la red y causan un DOS (denegación del servicio) a otros dispositivos de la red. La amenaza tiene un comportamiento exponencial al ir creciendo la población de infectados. Tomado de Trend Micro y de la enciclopedia wikipedia.

Nota:
El término inglés *worm*, también tiene otra acepción dentro del mundo de la informática: Worm (de write once, read many), perteneciente a las tecnologías de almacenamiento de datos. No debe ser confundido con el de gusano informático. Tomado de la enciclopedia wikipedia.

La figura 1.3 muestra el diagrama de decisión para la identificación de los códigos maliciosos de los sistemas de información.

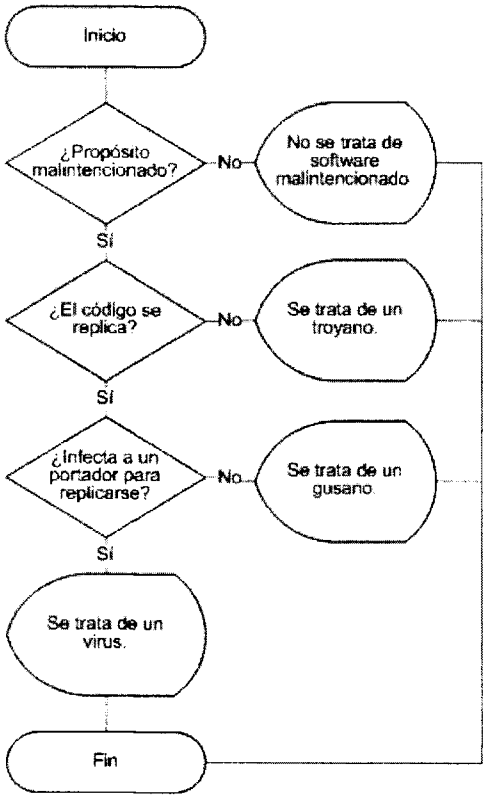


Figura 1.3 Árbol de decisión para determinar si se trata de código malintencionado
Fuente http://www.microsoft.com/spain/technet/recursos/articulos/avdind_2.mspx

1.5 Acotación del problema de amenazas de seguridad a los virus gusano (worms)

Organizaciones como CSI (Computer Security Institute), FBI (Federal Bureau of Investigation) y SANS (SysAdmin, Audit, Network, Security) comentan que del número importante de amenazas, los virus causan importantes pérdidas financieras y de productividad.

En este momento dado la importancia de problemas generados por los virus gusano (worms) se acota el tema de estudio de esta tesis a la investigación de los impactos económicos y de productividad originados por los virus gusano (worms).

El primer virus gusano (worm) de la historia fue el llamado Morris. Alrededor de la media noche del 2 de Noviembre de 1988 fue activado el worm Morris de 99 líneas de código, escrito por el estudiante de 23 años Robert Tappan Morris, y en horas sobrecargó servidores Unix alrededor del mundo.

Estos virus gusano (worms), impactan por explotar las vulnerabilidades conocidas de sistemas operativos muy comunes. Weaver y Paxson (2003) clasifican tres tipos de worms (self-carried, second channel y embedded). Generalmente encontraremos al segundo por atacar buffers en la computadora. Un estudio realizado en junio del 2002 revela que los diez principales casos de vulnerabilidades se presentaron en buffer/stack overflow ocupando las posiciones 1, 3 y 6 (Tevis y Hamilton, 2004).

Los virus gusano (worms) como mecanismos de negación de servicio presentan cuatro puntos importantes de ataque:

• **Cierres del sistema**. Si el software malintencionado consigue apagar o bloquear el sistema host, puede ocasionar problemas en uno o varios servicios. Para poder atacar el sistema host y hacer que se apague, el software malintencionado debe encontrar un punto débil en una aplicación o en el sistema operativo.

• **Inundación del ancho de banda**. La mayor parte de los servicios que se proporcionan en Internet están vinculados a través de una conexión de red de banda ancha limitada que los conecta a sus clientes. Si un creador de software malintencionado puede entregar una carga que ocupe este ancho de banda con tráfico de red falso, puede producir una denegación de servicio simplemente impidiendo que los clientes puedan conectarse directamente al mismo.

• **Denegación de servicio de red.** Este tipo de carga intenta sobrecargar los recursos disponibles para el host local. Recursos como el microprocesador y la capacidad de la memoria quedan saturados por los ataques del tipo inundación de paquetes SYN, en los que un atacante utiliza un programa para enviar múltiples solicitudes de SYN de TCP con el fin de llenar la cola de conexión pendiente en el servidor e impedir el tráfico de red legítimo a y desde el host. Los ataques del tipo bomba de correo también saturan los recursos de almacenamiento para crear un ataque DoS, en el que se envía a una dirección una cantidad excesiva de datos de correo electrónico en un intento de ocasionar problemas en el programa de correo electrónico o de impedir que el destinatario reciba otros mensajes legítimos.

• **Problemas en los servicios.** Este tipo de carga también puede ocasionar una denegación de servicio. Por ejemplo, esta técnica de ataque DoS tiene éxito cuando el ataque en un servidor de Sistema de nombres de dominio (DNS) deshabilita el servicio DNS. Sin embargo, puede que todos los demás servicios del sistema no resulten afectados.

Fuente http://www.microsoft.com/spain/technet/recursos/articulos/avdind_2.mspx

1.6 Cuantificación de las pérdidas económicas y de productividad a causa de los virus gusano (worms).

Existen varios datos documentados de pérdidas económicas muy importantes y de productividad a acusa de la amenaza de los virus gusano (worms). En este apartado se citarán algunas de ellas.

1. Cada año, organizaciones e individuos incurren a costos de miles de millones de dólares resultado de la pérdida de la productividad; generado principalmente por virus gusanos (worms) de computadora. Por ejemplo, el virus gusano Nimda infectó 2.2 millones de computadoras causando pérdidas por $370 millones. El virus gusano Loveletter causa pérdidas por $10 Billones y el virus gusano Melissa reporta daños por $385 millones (Neubauer y Harris, 2002).
2. La velocidad de propagación del virus gusano Sapphire (también conocido como Slammer) ha sido la más rápida de la historia ya que doblaba el tamaño de su propagación cada 8.5 segundos e infectó al 90% de los host vulnerables del mundo en 10 minutos (Moore et al, 2003). La figura 1.4 muestra las computadoras contaminadas 30 minutos después de ser liberado.

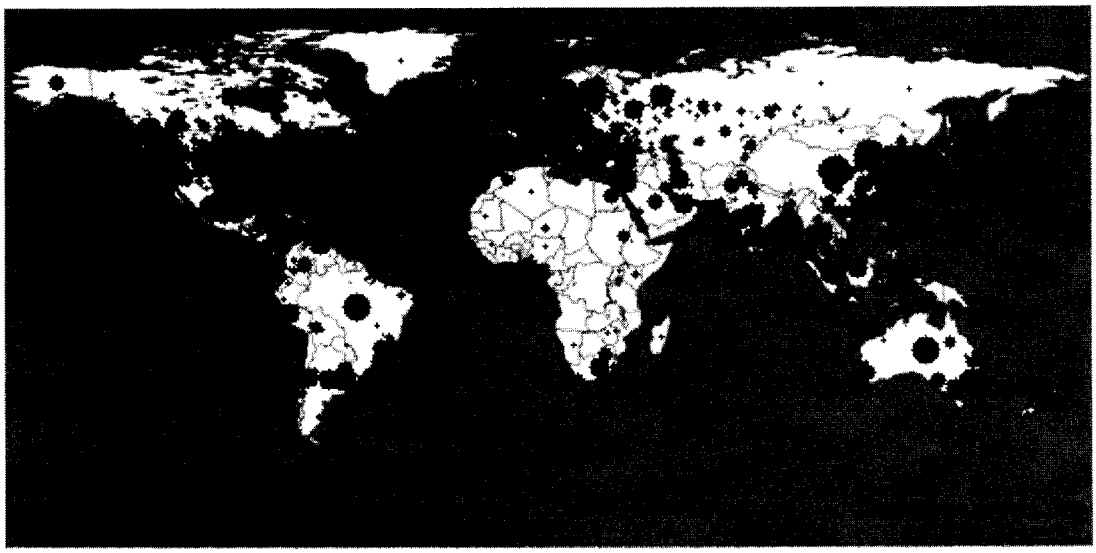


Figura 1.4 Propagación del virus gusano slammer 30 minutos de ser liberado.

3. En septiembre de 2003 datos no oficiales revelan cómo ante el máximo tráfico de enero por el virus gusano slammer, los administradores de las plantas eléctricas al norte de los Estados Unidos descuidaron sus firewall. Incubado 8 meses, en septiembre hay un apagón de varias horas en Nueva York, varios estados y Canadá (Krane, 2003). Otro virus gusano de alta propagación fue el CodeRedII ya que escaneaba bloques de redes al azar. Por último el virus SoBig produce un millón de copias en un periodo de 24 horas (fuente http://www.cisco.com/en/US/netsol/ns481/networking_solutions_white_paper0900aecd801e009f.shtml)

4. Congestión en enlaces, carga adicional en los servidores e incrementos de procesador en todos los dispositivos de interconexión de red. Trabajando con métricas de clientes de los proveedores de servicios (ISP) de Norteamérica, Sandvine Inc ha calculado que el ataque de los virus gusano (worms) (chicos o pequeños) han originado pérdidas al sector por más de $245 millones de dólares en el 2004.
5. IBM en noviembre del 2004 confirmó 997 ataques de Internet en septiembre dirigidos a redes que la compañía monitorea, que representan un aumento del 27% con respecto a los ataques de Internet confirmados en julio y agosto. Los ataques más comunes fueron los de varios gusanos, como Sasser y Korgo, destinados a explotar la vulnerabilidad dentro de LSASS, un componente de seguridad del sistema operativo de Microsoft Windows.

6. Mi2g Intelligence Unit ofrece estimados costos de los siguientes virus gusano (worms):
    a. Sobig: $37.1
    b. MyDoom: $22.6
    c. Klez: $19.8
    d. Mimail: $11.5
    e. Yaha: $11.5
    f. Swen: $10.4
    g. Love Bug: $8.8
    h. Bugbear: $3.9
    i. Dumaru: $3.8
    j. SirCam: $3

* En billones de dólares

El costo de los virus computacionales y gusanos podría ser más alto de lo que anteriormente se ha expuesto. Acordando con las nuevas estadísticas realizadas en Reino Unido indica que es la principal actividad de retraso de productividad del departamento de IT. The Corporate IT Forum conformado de 140 miembros indica que cada incidente está costando en promedio 122, 000 horas hombre y costos adicionales (Roberts, 2003)

Adicionalmente The Corporate IT (tif) hizo un estudio de los daños de los gusanos Welchia/Blaster de agosto del 2003. Tres cuartas partes de de los encuestados revela pérdidas de esfuerzo por 365 horas hombre en el departamento de IT y adicionalmente el 35% de estos mismos encuestados revela una baja en la productividad de toda la empresa en promedio de 3080 horas hombre. (Roberts, 2003)

Notas de periódicos ya empiezan a numerar los acontecimientos de virus gusano; por ejemplo; la Crónica de la Ciudad de México argumenta sobre información revelada por Trend Micro (casa de firma de antivirus) que 24 de 25 alertas amarillas emitidas fueron provocadas por algún ejemplar de las familias Sasser, Netsky, My Doom y Beagle. Adicionalmente la principal amenaza a la que se enfrentaron los usuarios de Internet fueron los gusanos, que supusieron 70 de cada cien incidencias relacionadas con virus. (Nova, 2005)

Las tendencias seguirán de estos acontecimientos. Lionel Phang, director y gerente de Trend Micro, afirmó que "el impacto económico y financiero de los ataques de los virus continuó aumentando en el año 2004"

1.7 Motivación de la investigación de tesis

Las universidades en sus inicios no fueron diseñadas con una estrategia de seguridad. Se pretende conocer qué análisis de seguridad realizan, cuáles son sus estrategias y cuántos son sus problemas en seguridad particularmente con los virus gusano (worms).

Los virus gusano (worms) por si solos provocan problemas de seguridad en la información, pero además pueden estar acompañados o venir con otros códigos maliciosos (malware). Se intenta integrar conceptos de la maestría de tecnologías de información en especial el enfoque de negocio y técnico, para realizar un método que contemple análisis de seguridad objetivo y robusto con las principales recomendaciones internacionales de seguridad en las empresas. Se pretende no sólo apoyar la gestión de la amenaza de los virus gusano (worms) si no que el método pudiera ser utilizado en otras amenazas de códigos maliciosos (malware).

Finamente existe la inquietud de romper los paradigmas de que las universidades no pueden aplicar la seguridad a niveles más aceptables o comparables con otras empresas.

1.8 Objetivo

Diseñar un método que permita prevenir y detectar la propagación de virus gusano (worms) para mitigar el impacto económico y mantener la productividad al ser implementado en las universidades de México.

1.9 Hipótesis

Los virus gusano (worms) al propagarse en la red de una universidad impactan económicamente a la institución educativa y reducen la productividad de las actividades en una computadora.

Es implícito que si es válido este modelo explicativo, la prevención y detección reducirá el impacto económico y mantendrá la productividad.

Las universidades de México no cuentan con las medidas de seguridad y análisis que se sugieren en la consultoría a empresas sobre seguridad informática.

En la figura 1.5 se detalla la concepción general de la problemática a estudiar.

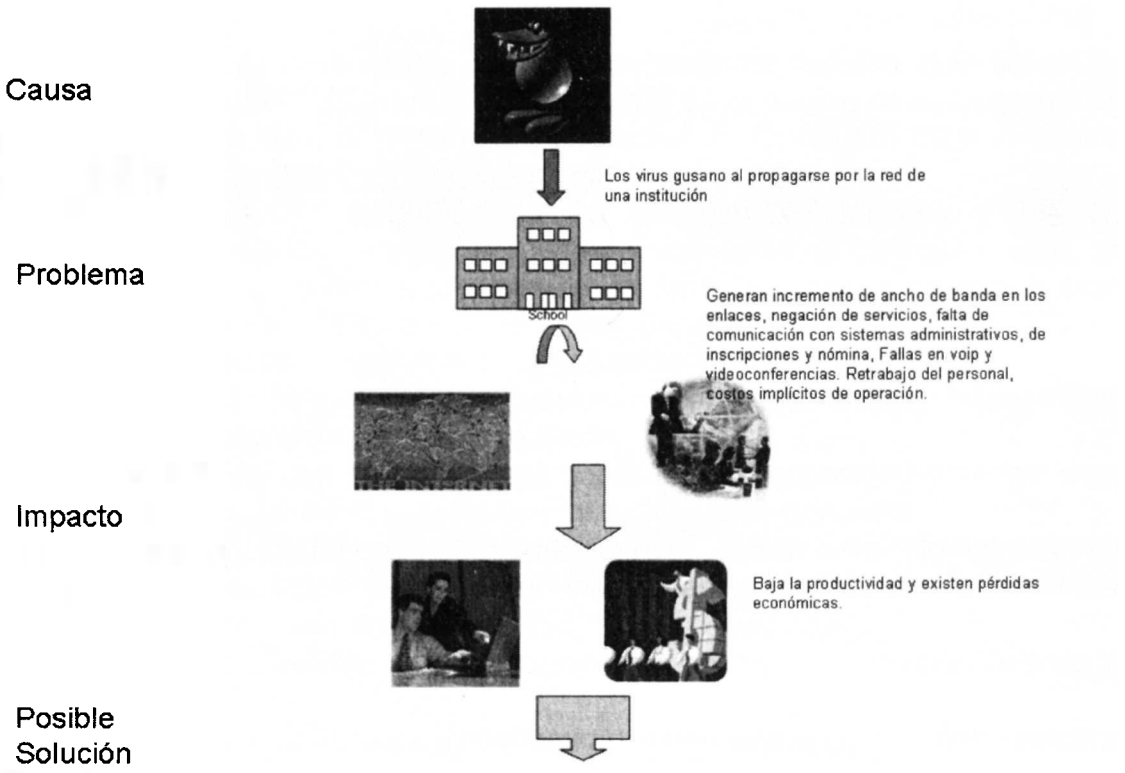


Figura 1.5 Resumen del planteamiento de trabajo de la tesis.

1.10 Alcance

- El estudio será realizado en universidades de México que tienen la infraestructura de Internet 2 contempladas en la página de la Corporación Universitaria para el desarrollo de Internet A. C. (CUDI) cuya dirección electrónica es http://www.cudi.edu.mx/
- Específicamente se selecciona 33 afiliados académicos y los 20 asociados académicos, contemplando únicamente un campus o sede en las universidades que tienen mas de un punto de presencia, salvo el caso del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) el cual se realiza un estudio completo de todos sus campis.
- Se trabajará con virus gusano (worms) es decir; todo lo que no tenga este comportamiento en virus será excluido.
- La plataforma que se investigará sobre su susceptibilidad ante los virus gusano (worms) es el sistema operativo Microsoft Windows.
- Quedan excluidos ataques sofisticados como escalamientos de privilegios, ataques dirigidos con herramientas de hackers o lammers, ingeniería inversa y social.
- La cantidad y calidad de información está sujeta a la disponibilidad de la misma.
- Los factores estratégicos y económicos están sujetos a la cuantificación o apreciación de los mismos por parte de las universidades en cuestión.
- Las encuestas serán realizadas a personal de tecnologías de información (directivos y administradores de red y computadoras) con poder de decisión.
- Las preguntas de la encuesta tratan de sondear si se realizan o no los análisis propuestos en las universidades. Se pretende adicionalmente conocer los puntos importantes para los encuestados de los análisis propuestos. Existe confidencialidad en los nombres de los encuestados y universidades.
- El estudio se limita a explorar si lo propuesto se usa o no, y puede o no ayudar a las universidades de México. Se pretende en un estudio posterior seleccionar a una universidad de México y realizar el método para comprobar su eficacia en un estudio de campo.
- El estudio de la seguridad informática es importante pero al igual delicado por la exposición de información que pudiera comprometer a la institución. La tesis no revela este tipo de información ni compromete a terceras personas.

1.11 Producto final

Al finalizar el desarrollo de la tesis, se contará con un método dirigido a las personas de tecnologías de información y al personal directivo de las universidades de México, campis del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) y miembros activos de la Corporación Universitaria para el desarrollo de Internet A. C. (CUDI), interesadas en ofrecer un ambiente mínimo de incidentes causados por los virus gusano (worms). Este modelo se basa en la prevención, detección y acción para poder mitigar el impacto económico que estos virus gusano (worms) originan y mantener la productividad en las actividades que se realizan con una computadora.

1.12 Contribución esperada

La contribución esperada consta de dos partes, un método que permita a los directivos de las universidades de México tomar la seguridad informática en términos de negocio y de conciencia de riesgo, teniendo presente los costos de oportunidad, de productividad y de inversión. Y dos, citar medidas de prevención y detección que sean eficaces, proactivas y que ayuden al personal técnico para minimizar la amenaza de los virus gusano (worms).

Existe además, una deducción, objetiva y de comparaciones muestrales para contrastar el panorama de los virus gusano (worms) en tres segmentos de estudio. La teoría muestra el cómo la industria, la consultoría y algunas universidades de Estados Unidos encaran el problema de los virus gusano (worms) y en general de la seguridad informática. Una especial contribución es hacer un cambio en la forma de pensar en la seguridad informática en general de las universidades de México.

1.13 Requerimientos para la institución educativa a quien va dirigido el método

- Miembros activos de la Corporación Universitaria para el desarrollo de Internet A. C. (CUDI).
- Tener un número importante de máquinas conectadas en red (mayor a 200) y que sean móviles; es decir no se encuentran en un espacio controlado.
- Tener enlaces de Internet 2 y de Internet dedicados y de un ancho de banda grande.
- Ofrecer modelos educativos que se sustenten parcial o completamente en plataformas tecnológicas y sistemas de información.

1.14 Requerimientos para la institución educativa para implementar el método

- Disponibilidad para realizar las mediciones, análisis y asesoría en el aspecto de negocio y técnico.
- Acuerdos de confidencialidad de la información entre el asesor y los asesorados y el personal de implementación.
- Integración de personal dueño, usuario y administrador de la información.
- Dedicación y continuidad para concluir los puntos del método.
- Adquirir la infraestructura que dicte el plan de acción y los análisis de retorno de inversión para medidas pequeñas o de importante capital para la minimización del impacto de los virus gusano (worms).
- Enfoque centrado en los procesos, personas y arquitectura (tecnología).
- Establecer una administración de proyectos para definir responsables, tiempos y la implementación del método.

1.15 Organización de la tesis

El estudio de tesis se encuentra estructurado en seis capítulos los cuales se representan en la figura 1.6

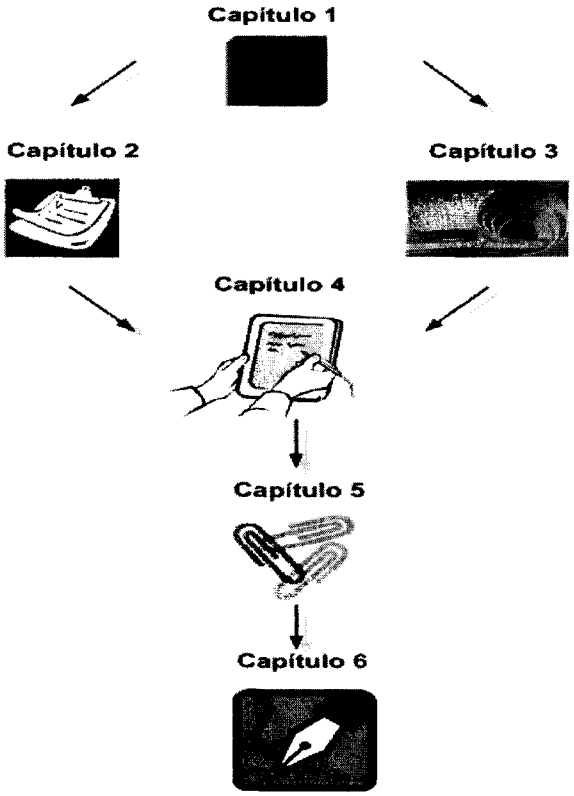


Figura 1.6 Organización del estudio de tesis.

El capítulo 1, nos presenta un panorama general de las amenazas informáticas y cómo interfieren en los sistemas de información. Posteriormente se limita a hacer un estudio de los virus gusano (worms) en sus impactos en la productividad y económicos. A continuación se pretende hacer una atención a la seguridad por parte de las universidades para entonces definir objetivo, alcance, intención, contribución y producto final del estudio.

En el capítulo 2 encontramos el diseño del método que permita prevenir y detectar la propagación de virus gusano (worms) para mitigar el impacto económico y mantener la productividad en las universidades de México. Se trabaja enfoques de negocio y técnico, actividades proactivas y reactivas, soluciones de código abierto y comerciales y soluciones no especializadas y muy especializadas.

Teniendo un método para poder minimizar el impacto de los virus gusano (worms), los consultores, investigadores y expertos en seguridad coinciden en que para todo trabajo de seguridad informática en general, debe de estar acompañado y amparado por una política de seguridad. Haciendo una analogía, el capítulo 2 ofrece cómo tener una policía preparada, objetiva, solvente, sustentable y que apoye a la comunidad pero debe de tener una constitución y leyes que normen sus actividades y que los apoye desde los mandos más altos. El capítulo 3 nos ofrece cómo iniciar a grandes rasgos con una política de seguridad.

El capítulo 4 se centra al conocimiento del trabajo de exploración en algunas de las universidades de México acerca de las aportaciones que ofrece el método propuesto. Se pretende indagar si los elementos propuestos en los capítulos 2 y 3 con utilizados por las universidades de México y si no los manejan revisar los puntos que consideran importantes que contengan estos elementos. La metodología y selección de población encuestada también se trabaja en este capítulo.

Los resultados del estudio del capítulo anterior son presentados en el capítulo 5 haciendo contrastes entre los campis grandes y medianos-chicos del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), además de las demás universidades de México asociadas al CUDI.

El capítulo final es el número 6 donde se presentan las conclusiones, los trabajos posteriores y las inquietudes por una seguridad en las universidades de México. Se pretende dar pauta a una continuación de la investigación para realizar el método propuesto en una universidad de México y poder generar un trabajo posterior.

Capítulo 2

Propuesta de diseño del método

Las universidades venden, por llamarlo así, educación como producto y servicio de una industria. El Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) ha incursionado además de modelos tradicionales de educación (maestro-alumno) con modelos de educación a distancia y virtuales desde hace 15 años. Las tecnologías de información han apoyado a esta estrategia en sus videoconferencias, trabajo a distancia y colaborativo.

Recientemente, otras universidades como lo son la Universidad Nacional Autónoma de México (UNAM) y la Universidad de Guadalajara (UDG) están incursionando el modelo a distancia en sus modalidades virtual y en línea y comienzan a depender más de sus tecnologías de información.

Existen amenazas informáticas que pueden afectar al buen funcionamiento de los sistemas de información utilizados para la educación en estas universidades o próximas en ofrecer estas opciones de educación.

El presente capítulo pretende trabajar con minimizar la amenaza de los virus gusano (worms) en las universidades de México y crear medidas de trabajo formal de seguridad informática y de negocio que son utilizadas por consultoras de seguridad y otras empresas.

2.1 Contabilización de la productividad en términos económicos

Las redes de datos cada vez soportan más aplicaciones y usuarios haciendo éstas cada vez más grandes y más complejas (Stallings 1996). Ahora bien, las redes son utilizadas por los sistemas de información. El uso de tecnologías de información, en muchas maneras, es regularmente citado como uno de los "key drivers" para el incremento de productividad en el mundo. (Gunasekaran, Khalil, Mahbubur Rahman, 2003)

Arturo Servín, nos comenta un aspecto muy importante a analizar cuando se habla de la importancia de tener los sistemas en operación es el costo de las fallas en la red. Citando un ejemplo de la compañía Anixter; en una red de área local (LAN) con 200 usuarios y tres servidores asumimos que cada servidor y sus componentes tienen en promedio 98% de disponibilidad durante las horas de producción en cualquier año (10 horas por día, 5 días por semana). Esto no da un tiempo esperado de caída de 52 horas por año, multiplicado por los 3

servidores nos da 156 horas por año. Con 200 usuarios en la LAN, la pérdida máxima total en horas persona es de 31,200 horas por año. Si asumimos un salario promedio de $35,000 USD por empleado, con una carga de factor de beneficios del 25% el salario promedio con esto es ahora de $43,750 USD y $21.88 USD por hora, entonces $21.88 x 31,200 = $682,656 USD. Una estimación más realista es asumir un factor de carga de trabajo por empleado, este estimado indica el tiempo en que el empleado esta accediendo la LAN para efectos no triviales. Si se asume un 30% requerido, entonces el costo de falla es del $204,749 USD. (Servín, 2004)

Si en lugar de hacer el análisis tomando en cuenta las fallas y lo hacemos tomando en cuenta la lentitud de la red, entonces en una compañía en donde sus empleados pierdan cada uno 5 minutos esperando a que se cargue la aplicación, esto nos da 21.67 horas por empleado cada año. Para el ejemplo anterior se traduce en una pérdida de $208.33 USD por empleado por año dando un total de pérdida de $20,833.33 USD de pérdida en la producción para la compañía. Pero el ejemplo no queda ahí, si calculamos una generación de ganancias por minuto de la compañía, esos 5 minutos se convierten en $2,083.33 USD de pérdida en las ganancias. Al año se pierden $104,166,67 USD en ganancias y $20,833 USD en producción, siendo la pérdida total de la compañía en $125,000 USD al año por tiempos lentos de la red. (Servín, 2004)

Según Gartner (2002) las tendencias para las aplicaciones de negocios, tendrán una evolución a una empresa virtual; permitiendo una colaboración ágil y orientada al tiempo real, enteramente enfocada a "core competencies". Lo anterior, nos puede sugerir que las universidades se enfocarán a hacer lo que saben "hacer" (enseñar) y dependerán de una productividad importante en sus sistemas de información.

La productividad perdida impacta a una organización ya sea industria o universidad. El virus gusano (worm) MS Blaster logró importantes pérdidas en universidades de Estados Unidos y México.

2.2 Productividad en términos de una universidad

De acuerdo al departamento de Information Technology Systems and Services (ITSS) de la universidad de Stanford, el virus gusano MS Blaster tuvo un impacto de $1.5 Millones de dólares en tiempo gastado para desinfectar computadoras. Los costos mas recientes de otro virus gusano (el Gaobot) fueron estimados en $0.5 millones de dólares.

Los costos anteriores directamente impactados a la productividad fueron acompañados por:

- Pérdidas de datos reformateando los discos duros después del ataque de los virus gusano (worms).
- Tiempo gastado por los Residential Computer Consultants y el departamento ITSS de Stanford para atender a usuarios infectados.
- Congestión de red por numerosos correos electrónicos (mails) mandados por computadoras infectadas y teniendo éstas que ser separadas del resto de la red del campus.
- Se tuvo que poner infraestructura adicional para filtrar correos electrónicos (mails), pérdida de la productividad por borrar dichos correos.
- Caída de la red. Downtime.

En México el panorama no fue diferente. El departamento de servicios de redes y telecomunicaciones de la Vicerrectoría de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) tiene documentado como impactó el virus MS Blaster en todos sus campis.

Durante dos semanas, se paralizó la red de impresión en casi todos los campis del sistema ITESM. La congestión de los enlaces hacia los diferentes campis y al Internet tuvieron varias caídas. Campus como Sonora Norte (Hermosillo) y León se colapsaron sus equipos de telecomunicaciones dejando de ofrecer servicios por horas. El personal directivo no tenía la capacidad de gestionar estrategias de ayuda para la eliminación del virus gusano y se tuvieron dos impactos adicionales a la pérdida de la productividad y pérdidas económicas: el virus impactó en el primer día de clases del semestre agosto-diciembre del 2003 y se perdieron varias inscripciones a diplomados por no estar operando los sistemas de tesorería.

2.3 Método propuesto.

Dado al enfoque de productividad, de actitud reactiva y proactiva ante los virus gusano (worms) y de usar estrategias y análisis robustos para la seguridad informática, se propone el siguiente método con bases sustentadas con diferentes consultoras de seguridad y de estándares. La figura 2.1 muestra el método propuesto en este estudio de tesis.

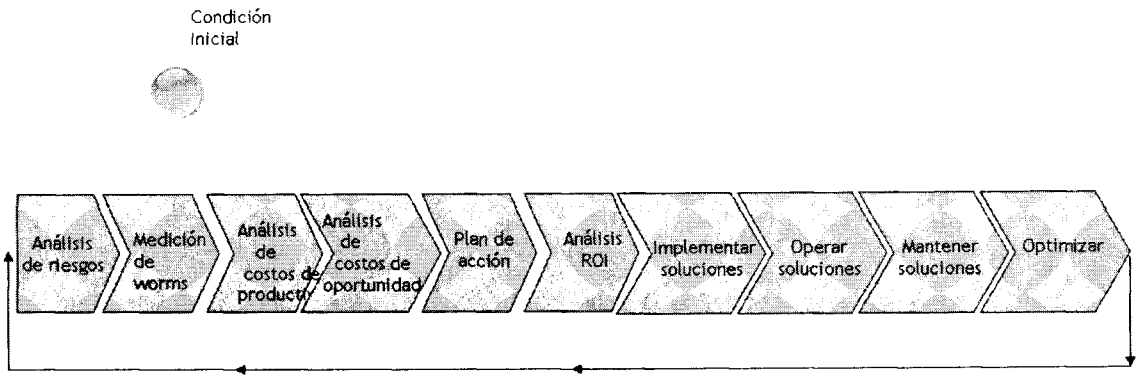


Figura 2.1 Método propuesto en el estudio de tesis.

Se propone un método de 10 pasos con requerimientos en cada eslabón que ofrezcan una entrada, un cómo y una salida. Al término del último eslabón, se buscará una capacidad de mejora en una siguiente iteración del método.

2.4 Comentarios para poder realizar el método propuesto

¿Qué se necesita para que funcione el método propuesto?

En primer instancia que se realicen los pasos, segundo contar con el respaldo de política de seguridad de la universidad que incluya al personal operativo, media gerencia y alta gerencia para que se pueda realizar lo propuesto, tercero tener líderes de la iniciativa de seguridad con las siguientes características: integrar el equipo, autoridad, poder e influencia (Arámbulo, 2005) y por último, se tenga una visión sistémica en los integradores de la solución y que además la gerencia con objetividad, conserve esta visión.

2.5 Desglosando el método propuesto

2.5.1 Punto 0. Condición inicial.

En este momento, sus sistemas de información, su seguridad, sus usuarios y fuentes de riesgo se encuentran, por decirlo así, en un punto inicial. Una condición en la que se espera "pase algo para cambiar de estado" ya sea bueno o malo. El método inicia con la contemplación de este entorno.

2.5.2 Punto 1. Análisis de riesgos.

Se contempla:

Una entrada: Necesidad de minimizar la amenaza de virus gusano (worms).

Un proceso: Identificar, analizar y administrar las fuentes de riesgos originados por los virus gusano (worms) y que afectan a la operación de la universidad.

Una salida: Un documento (análisis de riesgos) con un análisis cuantitativo y cualitativo de las amenazas y vulnerabilidades de los activos ante virus gusano (worms).

2.5.3 Punto 2. Medición de virus gusano (worms).

Se contempla:

Una entrada: Documento de análisis de riesgos.

Un proceso: Cuantificar el impacto de virus gusano (worms) usando las métricas: a) Inundación del ancho de banda, b) Máquinas vulnerables, c) Denegación de servicio de red y d) Downtime de los sistemas.

Una salida: Un documento con un análisis de la cuantificación de las métricas planteadas.

2.5.4 Punto 3. Análisis de costos de productividad

Se contempla:

Una entrada: Documento de cuantificación de virus gusano (worms).

Un proceso: Cuantificar el impacto de virus gusano (worms) usando las métricas: a) Relación tiempo/costo de técnicos en reparar equipo, b) Pérdida de información en equipo con virus gusano (worms), c) Relación tiempo/productividad por no realizar actividades.

Una salida: Un documento con un análisis de costos.

2.5.5 Punto 4. Análisis de costos de oportunidad

Se contempla:

Una entrada: Documento de análisis de costos.

Un proceso: Estimar el impacto de virus gusano (worms) en la disponibilidad de recursos que pudiera impedir una entrada económica a la universidad usando alguna métrica como: a) Ofrezco un diplomado y el sistema de tesorería no está disponible para hacer un pago.

Una salida: Un documento con una estimación de los costos de oportunidad.

2.5.6 Punto 5. Plan de acción

Se contempla:

Una entrada: a) Documento de análisis de riesgos.
b) Documento de cuantificación de virus gusano (worms).
c) Documento de análisis de costos.
d) Documento de análisis de costos de oportunidad.

Un proceso: Diseño de acciones preventivas y reactivas para minimizar el impacto económico de los virus gusano (worms) y mantener la productividad de la universidad.

Una salida: Documento de acciones preventivas y reactivas en un esquema paulatino y sustentable que integra actividades/procedimientos, personas y tecnología.

2.5.7 Punto 6. Análisis de retorno de la inversión (ROI)

Se contempla:

Una entrada: Documento de acciones preventivas y reactivas.

Un proceso: Cuantificar el plan de acción en costos y viabilidad económica.

Una salida: Un documento con un análisis de la cuantificación de costos tomando en cuenta el ROI, NPV (costos de operación e inversión) de actividades/procedimientos, personas y tecnología.

2.5.8 Punto 7. Implementar las soluciones

Se contempla:

Una entrada: Documento de acciones preventivas/reactivas y documento de análisis ROI.

Un proceso: Implementar el plan de acción con base a personas, actividades/procedimientos y tecnología.

Una salida: Documento de operación y mantenimiento de la solución planteada.

2.5.9 Punto 8. Operar las soluciones

Se contempla:

Una entrada: Documento de operación y mantenimiento de la solución planteada.

Un proceso: Operar el plan de acción con base a personas, actividades/procedimientos y tecnología.

Una salida: Documento de mantenimiento de la solución y de cuantificación de la efectividad.

2.5.10 Punto 9. Mantener las soluciones

Se contempla:

Una entrada: Documento de mantenimiento de la solución y de cuantificación de la efectividad.

Un proceso: Asegurar la operación continua.

Una salida: Documento de observaciones, retroalimentación y mejoras a una nueva solución.

2.5.11 Punto 10. Optimizar

Se contempla:

Una entrada: Documento de observaciones, retroalimentación y mejoras a una nueva solución.

Un proceso: Automatización y mejora de lo implementado, operado y mantenido.

Una salida: Generar los puntos de mejora de la fase iniciada (10 puntos) y retroalimentación a un nuevo análisis de riesgos.

2.5.12 Comparación costo-beneficio

Al término del método, la universidad se encontrará en otro estado, los sistemas de información, sus usuarios y sus fuentes de riesgo deberían de haber cambiado. Al contemplar de nuevo su entorno con respecto a los virus gusano (worms) en esta condición final, se propone hacer el análisis objetivo de los cambios. El beneficio es igual a la comparación entre el estado final y el estado inicial. Existió un esfuerzo económico, tecnológico, educativo y de actividades/procedimientos. ¿Valió la pena el esfuerzo? Al final del método, ¿fue igual, menor o mayor el problema de los virus gusano (worms)? La comparación costo-beneficio resaltará las áreas de oportunidad o apoyará la nueva iteración del método.

2.6 Análisis de riesgos

La palabra riesgo se deriva del italiano antiguo *risicare* que significa atreverse, en este sentido, el riesgo es más una elección que un destino.

Es importante tener la contemplación de que no existe nada 100% seguro y que necesitamos gestionar el riesgo en nuestra universidad.

Algunas opiniones importantes con respecto a la gestión de los riesgos son referenciadas en:

- El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy bien armados y pagados. Aún así, no apostaría mi vida por él. - Eugene Spafford. Extraído de http://www.ci.ulsa.mx/~elinos/docencia (Elinos, 2005).
- En la vida todo es administrar el riesgo, no eliminarlo. Walter Wriston, Ex-presidente de Citicorp
- "Se requiere una válvula que no tenga fugas y se intenta todo lo posible por desarrollarla. Pero el mundo real nos proporciona una válvula con fugas. Se tiene que determinar qué tanta fuga se puede tolerar" Arthur Rudolph, Científico que desarrollo el cohete Saturno 5, primer misión Apolo a la luna.

2.6.1 Realización de un análisis de riesgo

Un análisis de riesgo consiste en lidentificar, analizar y administrar las fuentes de riesgos antes de que empiecen ha amenazar el funcionamiento continuo y confiable de los sistemas de información (Labbé,2004).

Existen varias fuentes de riesgo. Trabajando directamente con los virus gusano (worms) la firma de antivirus Trend Micro, nos informa que se pueden contraer por:

1 Por red a causa de vulnerabilidades del sistema operativo.
1. Por ejecutar archivos anexos por correo electrónico, troyanos, spam, spyware o phishing.
2. Aceptar archivos contaminados por mensajería instantánea.
3. Visualización de archivos gráfico con terminación .jpg.
4. Virus gusano contraídos por tecnología Bluetooth en los celulares.

Se requiere identificar, por otro lado, los activos de la organización para poder así cuantificar o cualificar, los riesgos para cada activo o tipo de activo, además del valor del activo en sí y el impacto potencial de incidentes de seguridad en la organización (Labbé,2004).

Un activo son aquellos componentes de la organización (tangibles e intagibles) que son parte del patrimonio de la misma y necesitan ser resguardados. Se pueden estructurar en 5 categorías (mc2consulting, 2005):

1. El entorno del Sistema de Información
2. El Sistema de Información
3. La propia Información.
4. Las Funcionalidades de la Organización
5. Otros Activos

Una amenaza (Threat) es una combinación del riesgo, la consecuencia del riesgo, y la posibilidad de que el evento negativo vaya a suceder. (mc2consulting, 2005).

En un análisis de activos se hace una clasificación de la siguiente manera: (McNamee,2004):

a) Activos Blandos (Soft Assets)
b) Activos Duraderos (Hard Assets)
c) Activos Críticos

No todos los activos consideran una misma criticidad (Academia Latinoamericana de Seguridad, 2005)

En el caso de la universidad la criticidad debe de estar enfocada a los sistemas de información que apoyan a la educación.

Algunas preguntas, como las siguientes, tratan de clarificar los tiempos de tolerancia y criticidad para la universidad. Los activos responsables toman valor y criticidad.

¿Cuánto cuesta perder llamadas importantes? (válido en telefonía IP y VOIP)
¿Cuántos minutos puede retrasarse una clase por videoconferencia por perder sesiones o tener degrado en video/audio?
¿Cuánto tiempo son tolerantes las impresiones en días críticos; por ejemplo en exámenes?
Si la tendencia actual es vender clases profesionales o de posgrado por Internet; ¿Cuánto puedo tolerar downtime en plataformas tecnológicas?
Si las inscripciones son remotas ¿cuánto tiempo debe de tolerar un alumno en el proceso de inscripción por retrasos fuera del proceso?

Ahora bien, no sólo la criticidad se relaciona con dinero y tiempo, hay que tener en cuenta adicionalmente la probabilidad de riesgo, la exposición de riesgo, la tolerancia al riesgo y la máxima tolerancia al downtime de los activos para tener una opinión objetiva de la clasificación:

Una frase común a la cual se suele recurrir es que *"Una cadena se rompe por el eslabón más débil"* lo mismo ocurre en materia de seguridad no importa que la seguridad para un activo sea alta si para otro esta es débil (Labbé,2004). Este comentario intenta cuidar todos los activos pero intensificando los esfuerzos con aquellos activos que son más críticos.

2.6.2 Tipos de Análisis de Riego

El Impacto puede ser **cuantitativo** (si representa pérdidas cuantitativas monetarias directas o indirectas); **cualitativo** con pérdidas funcionales (Labbé,2004)

El análisis cualitativo no asigna valores a los componentes del análisis, más bien, se orienta al escenario, identifica los tipos de problemas que pueden ocurrir y trabaja a través de un escenario para determinar el resultado, el cual indicará cuál es la seriedad de la amenaza y la sensitividad de los activos. Este análisis es menos subjetivo que el análisis de riesgo cuantitativo y permite la aplicación de las herramientas de análisis (Palma. 2005)

Un apoyo a metodología cualitativa para el análisis de riesgos es el uso del método Delphi. Enric Bas, un experto en el tema nos dice que el Método Delphi tiene las siguientes características generales:

1. Método exploratorio
2. Cuantitativo/cualitativo predominantemente el último
3. Opinión grupal
4. Virtual
5. Con expertos (no élite)
6. Anonimato
7. Proceso dirigido
8. Basado en retroalimentación
9. Consenso

Un ejemplo de tabla con metodología cualitativa lo encontramos en la tabla 2.1.

Amenaza	Severidad	Probabilidad Amenaza	Potencial Pérdida	Efectividad Medida1	Efectividad Medida2

Tabla 2.1 Tabla de metodología cualitativa.

Para la metodología cuantitativa nos valemos de fórmulas y conceptos de probabilidad y ocurrencia.

El análisis cuantitativo asigna un valor numérico independiente y objetivo a los componentes de la evaluación de riesgo y la valoración potencial de pérdida (Palma, 2005).

En este análisis se trabaja con definiciones importantes. Apoyándonos de de **Albion Research Ltd.** en su glosario de Disaster Recovery Planning (DRP) cuya página electrónica es http://www.albionresearch.com/disaster/glossary.php tenemos:

Maximum Tolerable Downtime (MTD)

La longitud del tiempo máximo que una función del negocio puede ser continuada sin causar daño irremediable al negocio. Funciones del negocio asociadas al servicio de cliente y la facturación tiene a menudo un MTD más corto.

Annualized Loss Expectancy (ALE)

La expectativa anualizada de pérdida: es la pérdida monetaria prevista que se puede esperar para un activo debido a un riesgo sobre período de un año.

Se define como: ALE = SLE * ARO
donde SLE es el Single Loss Expectancy y ARO es el Annualized Rate of Occurrence.

Annualized Rate of Occurrence (ARO)

La probabilidad que un riesgo ocurra en un año particular. Por ejemplo, si los datos del seguro sugieren que un fuego serio sea probable ocurrir una vez en 25 años, entonces el índice anualizado de la ocurrencia es 1/25 = 0,04.

Single Loss Expectancy (SLE)
La singular expectativa de pérdida (SLE) es la pérdida monetaria prevista cada vez que ocurre un riesgo. El SLE, Asset Value (AV), y exposure factor (EF) son relacionados con la fórmula:

SLE = AV * EF

Exposure

La condición de ser susceptible a la pérdida debido a una amenaza.

Exposure Factor

La proporción del valor de un activo que es probable ser destruido por un riesgo en particular, expresada como porcentaje. Por ejemplo, si el valor de un edificio sería reducido a partir del $1.000.000 a $250.000 por un fuego, el factor de la exposición para el riesgo del fuego al edificio es el 75%.

Risk Tolerance
La capacidad de una organización de sobrevivir las pérdidas se asoció a riesgos

Un ejemplo de una tabla cuantitativa la encontramos en la tabla 2.2

Activo	Riesgo	Valor del activo	SLE	ARO	ALE
Calificaciones					
Impresión					
Nómina					
Investigaciones					
Videoconferencia					
Plataformas tecnológicas					
Servidores					

Tabla 2.2 Tabla de metodología cuantitativa.

Un ejemplo que contempla tres amenazas de virus gusano (worms) lo vemos en la tabla 2.3

Amenaza	Vulnerabilidad	Riesgo	Impacto
WormSasser		1. Congestión de tráfico en la red. 2. Reinicio de la máquina con worm en determinados periodos de tiempo.	1. Aplicaciones sensible con retardo. 2. Voip y Telefonía ip con interrupciones. 3. Mala calidad en las videoconferencias de clases.
WormBlaster		1 .Congestión de tráfico en la red. 2. Reinicio de la máquina con worm en determinados periodos de tiempo. 3. Problemas en compartir archivos en redes Microsoft. 4. Problemas en directorio activo de Microsoft.	1. Aplicaciones sensible con retardo. 2. Voip y Telefonía ip con interrupciones. 3. Mala calidad en las videoconferencias de clases. 4. Problemas para imprimir, compartir y firmarse a redes Microsoft.
WormSlammer		1. Congestión de 99% de la red. 2. Colapso en la gran mayoría de equipo activo de la red. 3. Falta de conectividad a bases de datos Microsoft.	1. Paralización total de todas las actividades por red de la universidad.

Tabla 2.3 Análisis de riesgo de tres virus gusano.

2.6.3 Análisis de impacto al Negocio (Business Impact Análisis)

La consultora Profit de España comenta que si la operación del negocio depende de sus sistemas de información, en particular, a empresas de grandes dimensiones con alto grado de automatización de sus procesos de negocio se debe de tener un adecuado plan de análisis de riesgos:

- Una fase inicial de análisis de riesgos en caso de desastre, denominada **Business Impact Analysis (BIA).**
- Una fase posterior en la que se establece el plan para la mitigación de estos riesgos, denominada **Business Continuity Plan (BCP).**

El BIA tiene como objetivo evaluar el riesgo soportado por la organización, teniendo en cuenta los problemas potenciales que puedan afectar a su operación, y consiste en cuatro tareas principales:

1. **Selección de los procesos de negocio críticos** (para los cuales se pretende establecer una solución de recuperación en caso de desastre) y su respectiva Arquitectura de TI de soporte.
2. **Identificación de los niveles de servicio que necesitan ser garantizados para cada proceso** (a través de la evaluación del coste de la interrupción de los servicios y de la reposición de la información).
3. **Identificación de los desastres potenciales.**
4. **Evaluación del impacto** provocado, en cada proceso, por los diferentes tipos de Desastre y su probabilidad de ocurrencia.
5. **Definición de las medidas que precisan ser implantadas para reducir el riesgo** (Datos, Servidores, Centros de procesamiento, Locales de trabajo y comunicaciones) en base a un análisis de coste/beneficio.

2.6.4 Análisis de Continuidad del Negocio (Business Continuity Plan)

Una vez definida la solución de Continuidad del Negocio se hace necesario su desarrollo y puesta en práctica en la organización.

El Business Continuity Plan define la solución escogida por la organización como estrategia de recuperación de servicios y reposición de información en caso de desastre y establece las directrices de coordinación entre las partes involucradas para asegurar la recuperación cumpliendo los niveles de servicio establecidos.

Un Business Continuity Plan puede incluir varios tipos de documentos con objetivos distintos:

- **Plan de Recuperación de Desastres (DRP)** – Establece la estrategia de recuperación de las aplicaciones críticas, i.e., aquellas aplicaciones que soportan los procesos críticos del negocio.
- **Plan de Continuidad de Operaciones** – Establece el plan de recuperación de los procesos de negocio, a veces incluyendo procesos manuales alternativos.
- **Planes de Contingencia** – Establece alternativas en caso de que fallen las soluciones establecidas para la recuperación en caso de desastre debido a factores externos a la organización.

La figura 2.2 es un ejemplo de un Análisis de Continuidad del Negocio (Business Impact Analysis) más elaborado.

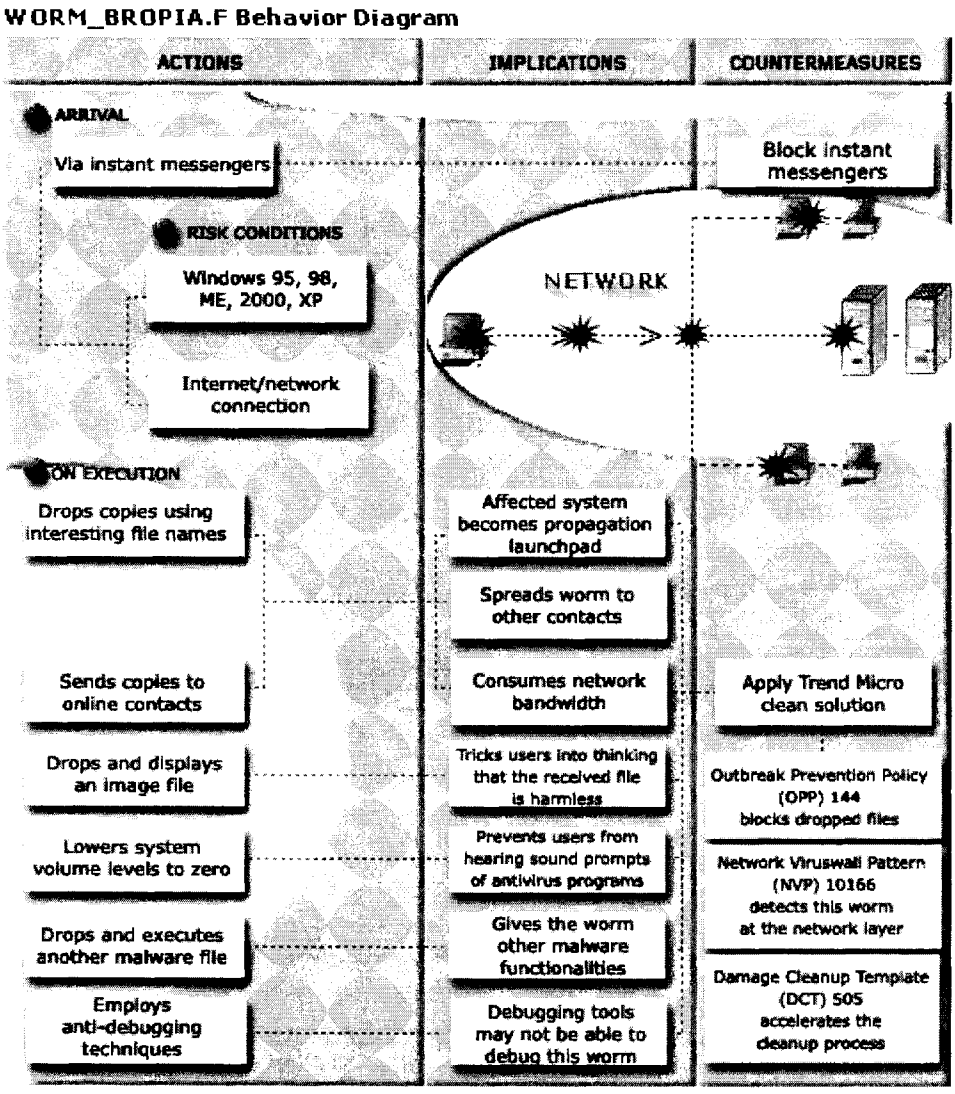


Figura 2.2 Análisis de Continuidad del Negocio (Business Impact Analysis) para el Worm Bropia tomado del Security Info de Trend Micro, febrero del 2005

2.6.5 Comentarios adicionales de un análisis de riesgo

En las tecnologías de información, parte de la seguridad informática es regulada con las metodologías o certificaciones de (isc) ², el detalle de cómo lograr un mejor análisis de riesgo sería conveniente consultar dicha organización.

(ISC)² (International Information Systems Security Certifications Consortium, Inc.) es una organización global sin ánimo de lucro de la que forman parte los más reconocidos expertos en seguridad de todo el mundo. Administra un examen conocido como (Certified Information System Security Professional) que refleja un conocimiento seguridad de la información en los rubros Access Control Systems, Cryptography, and Security Management Practices. Se pueden consultar sus páginas electrónicas en:
http://www.cissps.com/
https://www.isc2.org/cgi-bin/index.cgi

2.7 Medición de virus gusano (worms).

La medición es el primer paso para el control y la mejora. Si no se puede medir algo, no se puede entenderlo. Si no se entiende, no se puede controlar. Si no se puede controlar, no se puede mejorar" H, James Harrington

"Estudia el pasado si quieres pronosticar el futuro". Confucio (551-479 a. C.); filósofo chino.

Bruce Moulton consultor de Symantec en el 2004 comenta: el dicho antiguo "Lo que se mide se hace" se aplica aquí. De forma análoga, reafirmemos también lo contrario: "Lo que no se esté midiendo probablemente no se está haciendo".

Parte de la estrategia de la medición de virus gusano (worms) inicia con la contabilización de cuántos virus existen. El departamento de servicios de redes y telecomunicaciones de la Vicerrectoría de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) proporciona para el estudio, algunos campis en los cuales se muestra la relación de tráfico a enlaces entre los distintos campis y sistema ITESM, estos enlaces son para la comunicación con los servicios de educación como lo son las plataformas tecnológicas y las videoconferencias.

Definiendo un paquete de datos en red, como un contenedor de transmisión de datos tenemos una relación de cuántos paquetes entran al router y cuántos paquetes salen de éste dado que los demás fueron filtrados por tener virus gusano (worms).

La tabla 2.4 nos muestra la relación de paquetes de un campus hacia el sistema ITESM u otro campus. Por ejemplo, el campus León de cada 100 paquetes mandados 91 contienen virus y son filtrados. Las proporciones y el problema se acentúan dependiendo del tamaño de campus.

Campus	%Virus Blaster y familia	%Virus Sasser y familia	%Virus Slammer	%Todos los demás paquetes del campus.
Querétaro	37.5	18.5	0.014	43.986
Guadalajara	37.34	49.33	1.1	13.23
Toluca	13.23	34.56	1.3	50.91
León	0.74	89.28	0	9.98
Hermosillo	27.18	6.23	0	66.59
Irapuato	0.08	36.81	0	63.11
Mazatlán	9.13	34.34	0	56.53
Colima	0.09	0.02	0	99.89
Obregón	0.45	0.12	0	99.43
Culiacán	22.12	27.5	0	50.38
Puebla	13.2	83.1	0	3.7
Morelia	5.3	33.56	0	61.14
Hidalgo	0.04	59.4	0	40.56
Veracruz	0.1	94.12	0	5.78
Cuernavaca	16.33	81.065	0	2.605
Chiapas	9.05	56.71	0.0004	34.2396

Tabla 2.4 Relación de paquetes con virus en algunos campis del sistema ITESM.

En el anexo B de este estudio de tesis, se explica a detalle como hacer mediciones de tres tipos de virus gusano (worms).

Otro tipo de mediciones son las de la cantidad de máquinas que son "vulnerables" o susceptibles a contraer virus gusano (worms). Una herramienta que se localizó para la investigación y que se usa en el ITESM es scanlite. Scanlite que es un módulo en lenguaje perl diseñado por John Ballem de la Universidad de Brown para detectar máquinas con algunas vulnerabilidades conocidas. Se puede obtener este módulo en la dirección electrónica de http://www.cpan.org/

2.8 Análisis de costos de productividad

El análisis de costo de productividad tiene que ver en las actividades que se dejan de hacer por atender a anomalías en los sistemas de información o la computadora de los usuarios a causa de los virus gusano (worms). El diccionario de economía y finanzas en su página electrónica http://www.eumed.net/cursecon/dic/c13.htm define que la productividad del trabajo, se mide por la producción anual -o diaria, u horaria- por hombre ocupado: ello indica qué cantidad de bienes es capaz de producir un trabajador, como promedio, en un cierto período.

Las métricas que se proponen para relacionar la productividad son:

a) Relación tiempo/costo de los técnicos en reparar equipo.
b) Pérdida de información en equipo debido a los virus gusano (worms).
c) Relación tiempo/productividad por no realizar actividades.

La tabla 2.5 muestra un ejemplo de cómo determinar los costos en la productividad a causa de los virus gusano (worms).

Acontecimiento	Tiempo	Sueldo en min del técnico o usario	Frecuencia	Total
Descontaminar una máquina con worm				
Respaldo inminente de la información del usuario por causa de un worm				
Pérdida de información por causa de worms				
Tiempo en que no puede realizar sus actividades el usuario afectado.				

Tabla 2.5 Análisis del impacto a la productividad por realizar desinfección de los virus gusano.

2.9 Análisis de costos de oportunidad

El diccionario de economía y finanzas define que el costo de oportunidad de producir algo es igual al valor de las producciones alternativas a las que se renuncia para obtenerlo.

En términos de una universidad nos pudiéramos preguntar ¿cuánto he dejado de ganar por operaciones que no se pueden realizar debido a no estar disponibles? Por ejemplo, entrevistas al área de cajas, tesorería o el personal que tiene directamente que decir que el servicio no está disponible y que regrese después.

2.10 Plan de acción

Generalmente la frase después de ahogado el niño se tapa el pozo. El ser humano generalmente trabaja en forma reactiva en lugar de la proactiva. Un diseño de un método para poder hacer frente a los virus gusano (worms) deberá de constar de ambas partes y con un sustento importante en la política de seguridad propuesta en el capítulo 3.

David Harley, Robert Slade u Urs E. Gattiker en su libro virus informáticos comentas un estudio de los dos ámbitos anteriores.

Administración Proactiva: trabajo en estrategias, sistemas y administración de redes y desarrollo.

Administración Reactiva: atención a incidentes y acciones proactivas complementarias (técnicas, administración y educación).

Dado que es una estrategia de propagación de virus o worms el scanear (Briesemeister y Lincoln, 2003), recorrer redes secuencialmente, sería una medida efectiva el poder detectar nuestros puntos débiles antes que lo hicieran worms. Para este punto, un proceso proactivo en las universidades es un movimiento general en todo el mundo; en especial por el radical problema que los alumnos tienen computadoras vulnerables y no es fácil implementar políticas de seguridad como las aplicadas a las máquinas del personal de cualquier empresa. Se presenta la necesidad de crear métodos sociales, culturales y sencillos para evitar pandemias.

Básicamente, se trata de trabajar en dos modelos: el de epidemia y el de predador-presa. En el primero, existen dos estados: susceptibles e infectados (Zou et al, 2002) y se pretende reducir la posibilidad de que los primeros pasen

al estado de infectados. El otro modelo nos ayudará si es que existen infectados trabajar con: a) búsqueda de virus, b) eliminación de virus y c) multiplicación de los procesos predadores (Toyoizumi y Kara, 2002) para eliminar más rápido a la población de virus.

Después de conocer los modelos, se necesita un método para llegar al fin deseado. Comentarios de seguridad de David King (2003), quien es el director de mercadotecnia VPN y seguridad de Cisco System, en el libro de Hacking Exposed nos permite identificar 5 elementos claves en la seguridad: políticas, planes, productos, procesos y personas.

En el primer rubro señalado; es necesario el compromiso muy especial de los directivos y profesores de la universidad, ya que en gran medida, el poder controlar este problema tecnológico-social dependerá de sus decisiones y apoyos constantes en un proceso prioritario y de importancia. En materia de los planes es idóneo el poder tener organización, bitácoras de trabajo y estrategias de contingencia; entre las más representativas. Para los productos hay una enorme variedad; en los que podemos mencionar los esfuerzos de muchas universidades y de firmas comerciales como: los detectores de malware (Christodorescu y Jha, 2004) y de vulnerabilidades (como el Reggie de la univerisidad de Brown (Ballem, 2004)), software antivirus, detección de intrusos y portales de registros de la red.

Para una universidad y en general una empresa la población de máquinas es divida en dos segmentos: a) quienes pueden realizar ataques y b) quienes no tienen la remota idea de que hacen y causan grandes daños. Este último sector es por mucho, más de la mitad de la población. Por ejemplo, el sistema XP se encuentra instalado en 210 millones de máquinas en el mundo (Acohido y Swartz, 2004) y es el más vulnerable de todos. Y por otro lado, además de vulnerabilidades en las máquinas de alumnos, uno de los grandes problemas es que no cuentan con un software antivirus. Por ejemplo, el 78% de los incidentes respondidos en noviembre del 2000 por la universidad de Harvard terminaron con la instalación de antivirus (Davis, 2001)

Los procesos y personas son muy ligados ya que sin personas los procesos no pueden realizarse. Hay dos casos de universidades que presentan esfuerzos en materia de procesos y educación al usuario. El proyecto de documentación por web de la Universidad de Delaware que sustenta a su Help Center para informar y educar a los usuarios acerca de sus tecnologías y la forma de operarlas. (Hopkins, 2000) y el proyecto SOS (Service on Site) de la Universidad de Brown. Dado que en la gran mayoría de universidades hay dormitorios o residencias para los estudiantes; esta universidad tiene dos equipos de personas que dan soporte libre de cargo a los jóvenes que tienen un problema y que es complicado poderlo resolver con una llamada (Snyder, 2003).

Otro punto interesante a tomar en cuenta; es el Total cost of ownership (TCO) que busca cuantificar el costo de la organización por empleados, infraestructura, soporte en helpdesk, upgrades y mantenimiento en curso (Lei y Rawles, 2003). El poder reducir la incidencia de virus en nuestras redes nos permitirá bajar los costos de TCO y aumentar el "Service Level Agreements" (SLA) de éstos; en una nueva forma de compromiso llamada SSLA (Security Service Level Agreements) "acuerdos de nivel de servicio en seguridad" (Henning, 1999)

Como se ve en los puntos anteriores, hay un gran esfuerzo por parte de algunas universidades americanas (no son todas) por reducir el impacto dañino de los virus, pero se encuentra que son esfuerzos separados y que no se ve aun, a la seguridad universitaria como un sistema. Juan Manuel Ramos (2003) menciona algo muy acertado "existe la necesidad de gestionar la seguridad informática no como un estado sino como un proceso".

La investigación de tesis propone soluciones tecnológicas para minimizar el impacto de los virus gusano (worms) y que se pueden realizar inmediatamente, con implementación de códigos abiertos (open source) y con una inversión importante pero la solución es más robusta.

2.10.1 Soluciones técnicas preventivas

El trabajo preventivo se puede realizar con las siguientes soluciones y se listan en orden de complejidad, robustez e inversión:

Campañas de educación

Actualización del sistema operativo Microsoft Windows en la página electrónica:
http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us

Instalación de un firewall como en las opciones:
XP2 Firewall
http://www.zonelabs.com
http://www.symantec.com/region/mx/product/consumer/npf/
http://www.tinysoftware.com/home/tiny2?la=EN
http://us.mcafee.com/root/landingpages/affLandPage.asp?affid=101&lpname=linkshare_mpfp&cid=5616&siteID=qBNKIhsBsB4-mrqC0MygYfeoI6oXrSAt%2AQ

Uso de herramientas código abierto (open source) para detectar máquinas vulnerables.
http://www.cpan.org/

Instalación de un antivirus como en las opciones:
http://www.symantec.com/index.htm
http://us.mcafee.com/root/landingpages/affLandPage.asp?affid=101&lpname=linkshare_vso&cid=5617
http://www.pandasoftware.es/
http://www.trendmicro.com/la/home/enterprise.htm

Instalación de un antispyware como en las opciones:
http://www.microsoft.com/athome/security/spyware/software/default.mspx
http://www.safer-networking.org/es/download/index.html
http://www.lavasoft.com/

Actualización de paquetería office en la página electrónica:
http://office.microsoft.com/es-mx/officeupdate/default.aspx

Segmentación de la red física o lógica. En el caso de la segmentación lógica se le conoce como VLANS (virtual lan).

Registro de red de los usuarios:
http://www.netreg.org/
http://www.brown.edu/Facilities/CIS/Projects/netreg/reggie/
Dominio de microsoft acompañado de la solución Windows Server Update Services (WSUS).

Verificar que funcione adecuadamente su antivirus. Es posible que se tenga un antivirus pero no este trabajando correctamente, para ello se puede revisar si realmente realiza su labor con un test de antivirus en la página electrónica del European Institute for Computer Antivirus-Reseach http://www.eicar.com/anti_virus_test_file.htm#dl
Eicar provee un string de 68 caracteres que al ser puesto en un archivo llamado eicar.com debe crear una respuesta de cuarentena por parte del antivirus.

Soluciones Sybari de Microsoft: consultar su página electrónica: http://www.microsoft.com/windowsserversystem/solutions/security/sybari.mspx

Uso de tecnología de vlans dinámicas: Membership Policy Server (VMPS),
http://www.cisco.com/en/US/tech/tk389/tk814/tk839/tsd_technology_support_sub-protocol_home.html
http://linux.softpedia.com/progDownload/VMPS-Download-5028.html

Uso de tecnología Private VLANs.
http://www.cisco.com/en/US/tech/tk389/tk814/tk840/tsd_technology_support_sub-protocol_home.html

Cisco Secure Access Control Server (ACS)
http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

Cisco Network Admission Control (NAC)
http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

Extensible Authentication Protocol (EAP), 802.1x, y RADIUS.
http://www.cisco.com/en/US/products/ps6662/products_
http://www-128.ibm.com/developerworks/library/l-radius/

2.10.2 Soluciones técnicas reactivas

El trabajo reactivo se puede realizar con las siguientes soluciones y se listan en orden de complejidad, robustez e inversión:

Listas de acceso en equipo de telecomunicaciones

Uso de tecnología IDS (Sistema de Detección de Intrusos).

Uso de tecnología IPS (Sistema de Prevención de Intrusos).
http://www.ecs.utdallas.edu/ACE/pdf/charon_2005.pdf

Correlación de alarmas entre herramientas de monitoreo, IDS e IPS.

Monitoreo de peticiones de nombre por máquina al DNS (Servidor de solución de nombres).

Bloqueo de máquinas con virus gusano (worms); mandar a cuarentena.

Equipo especializado para detección de virus gusano:
http://www.trendmicro.com/la/products/eps/eps/evaluate/overview.htm

2.11 Análisis del retorno de la inversión (ROI)

La inversión de alguna solución técnica, de proceso o de personas pueden ser considerados en los análisis de retorno de la inversión y valor presente para tener en cuenta las opciones que se tendrán para minimizar el impacto de los virus gusano (worms) y cómo la recuperación de la inversión en un determinado periodo, además de contar con la apreciación o depreciación de los bienes que se adquieran.

El análisis de retorno de la inversión (ROI) (en inglés Return on Investment) comenta el porcentaje de inversión regresado anualmente para recuperar el monto inicial del proyecto. Además el valor de vida de la inversión. Para este caso de trabaja con medidas como el NPV (Schultz, 2004).

El valor presente neto (NPV) (en inglés Net Present Value) calcula el valor presente de cada flujo de efectivo en los proyectos y los adiciona a ellos. Introduce el "valor del dinero en el tiempo" en sus cálculos (Schultz, 2004).

2.11.1 Componentes del valor presente neto (NPV)

1. *Tasa de devaluación*: consideración del valor del dinero en el tiempo.
2. *Inversión*: el monto de iniciación del proyecto.
3. *Impacto en las ganancias*: durante la implementación del proyecto o iniciativa se presentará ganancias o pérdidas a la compañía.
4. *Impacto en los costos*: durante la implementación del proyecto o iniciativa se presentará reducción o incremento de costos en la compañía.

2.11.2 Fórmula del NPV

$$NPV = \sum_{t=1}^{n} (R_t - C_t) / (1+r)^t - I$$

Donde t es el tiempo, n el número de períodos, R el impacto en las ganancias, C es el costo del impacto, y r es la tasa de devaluación de la inversión.

Generalmente se toma un periodo de 5 a 10 años pero depende de cada empresa.

- Si se presenta un NPV positivo el proyecto es satisfactorio, y el valor de la empresa debe de incrementarse con dicho proyecto.
- Reglas de decisión:
  - NPV > 0 → aceptar el proyecto
  - NPV < 0 → rechazar el proyecto.
  - NPV = 0 → punto de quiebre entre aceptar o rechazar un proyecto.
  - Con mutua exclusividad de proyectos; seleccionar el que tenga más NPV.

Por último algunas consideraciones finales para el NPV y ROI en un proyecto son (Schultz, 2004):

1. Crear escenarios donde se contemple el mejor y peor caso del proyecto.
2. Identifica Impacto estratégico. Entendiendo e identificando las ventajas estratégicas y los costos asociados a la puesta en práctica de la iniciativa o proyecto puede ser dominante a ganar ayuda para su aprobación.
3. Mantenga un margen de error. Tener holgado la inversión del proyecto hará que sea menos susceptible a riesgos imprevistos.
4. Los accionistas deben de tener seguro el proyecto como un mecanismo estratégico que ayude a lograr tener la compañía más competitiva.
5. Realizar una documentación detallada en el proceso de inicio e implantación del proyecto para comparar lo proyectado con lo real. Inversión, interés, impactos reales en costos pueden dar una retroalimentación para futuros proyectos.

2.11.3 Preguntas importantes acerca del ROI y NPV

¿Puede la iniciativa ser instalada o el proyecto ejecutado según lo diseñado sin la inversión propuesta o se pudiera sustituir con otro recurso?

¿Si este proyecto o iniciativa se retrasa por un año, este costo será evitado o este recurso estará disponible para otro propósito?

Es así que adicionalmente al análisis NPV y ROI, un proyecto exitoso comienza primero con una filosofía de negocios que pueda alinear a la empresa, sus empleados, y sus sistemas alrededor de las necesidades de los consumidores, y lejos del modelo tradicional enfocado en los productos o procesos. Una exitosa implementación de un proyecto siempre cuenta con el apoyo de la alta dirección e involucra a toda la empresa. La Tecnología es solo un complemento que sirve para apoyar todos estos cambios, no es la solución por si sola (Pedemonte, 2005)

2.12 Implementar las soluciones

Implementar el plan de acción con base a personas, actividades/procedimientos y tecnología.

2.13 Operar las soluciones

Operar el plan de acción con base a personas, actividades/procedimientos y tecnología.

2.14 Mantener las soluciones

Asegurar la operación continua.

2.15 Optimizar las soluciones

Mark E. Egan Gerente de Información y Vicepresidente de Tecnología de la Información de Symantec Corporation comenta que los programas de seguridad de la información no son para implementar y luego dejar en piloto automático. Así como las amenazas a la seguridad y la tecnología nunca se detienen, la curva de aprendizaje de sus empleados tampoco debe estancarse. Certificaciones importantes sobre lo más nuevo en seguridad y en este caso reducción de virus gusano (worms) pueden ser las siguientes:
Certified Information Systems Security Professionals (CISSP)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
SANS Global Information Assurance Certifications (GIAC)

Capítulo 3

Diseño de una política de seguridad

En el capítulo anterior, se realizó una presentación de los acontecimientos de amenazas informáticas y la forma en que los virus gusano (worms) pueden ser tratados para minimizar su impacto económico y de productividad en las universidades de México. Se pretende que al conocer las amenazas y después, creando una analogía, el diseño de una policía preparada, objetiva, solvente, sustentable y que apoye a la comunidad, sería importante tener las leyes, legislaciones o constitución para normarla; en términos de seguridad informática se le conoce como política de seguridad.

En este capitulo, se atenderá la necesidad de un diseño de política de seguridad y una propuesta de conceptos clave para iniciarla.

3.1 Inicio del concepto de política de seguridad

Juan Ignacio Ruiz (2004), consultor de México Channel Manager y socio de Internet Security System, comenta que se debe de tomar en cuenta que el problema de la seguridad se encuentra en dos ámbitos:

Administrativo

- Gerencia.
- Políticas de seguridad.
- Concientización.
- Capacitación.
- Análisis e informes – Estadísticas.

Técnico

- Monitoreo de redes.
- Análisis de vulnerabilidades.
- Control y respuesta a incidentes.

Igualmente la academia Latinoamericana de Seguridad Informática (2005) comenta que el problema consiste en dos partes: la tecnológica y la humana. Y siendo en las dos un pilar importante la administración para regularlas.

En su libro Security architecture: design, deployment and operations, Christopher King y colaboradores (2001) muestra que estás dos opiniones se encuentran en una parte importante en su pirámide de seguridad mostrada en la figura 3.1

Figura 3.1 Modelo de seguridad propuesto por King et al. 2001

La seguridad informática, nos lleva a pensar que su implementación no es solución mágica para resolver las amenazas informáticas (CA Computer Associates, 2004) sino todo un proceso.

Dicho proceso involucra a todos los miembros de la organización y teniendo en cuenta que las decisiones de seguridad vengan de la alta gerencia y no del departamento de tecnologías de información (TI) (Cisco Networkers Acapulco México, 2004).

Con base a lo anterior, un reto especial es lograr que la alta gerencia tenga claro los objetivos de negocio y de seguridad informática. El Seminario de seguridad Cisco realizado el 17 y 18 del febrero 2005 ejemplifica en la figura 3.2 el concepto actual y real de lo que piensan algunos gerentes de empresas e inclusive los directores de tecnologías de información (TI) .

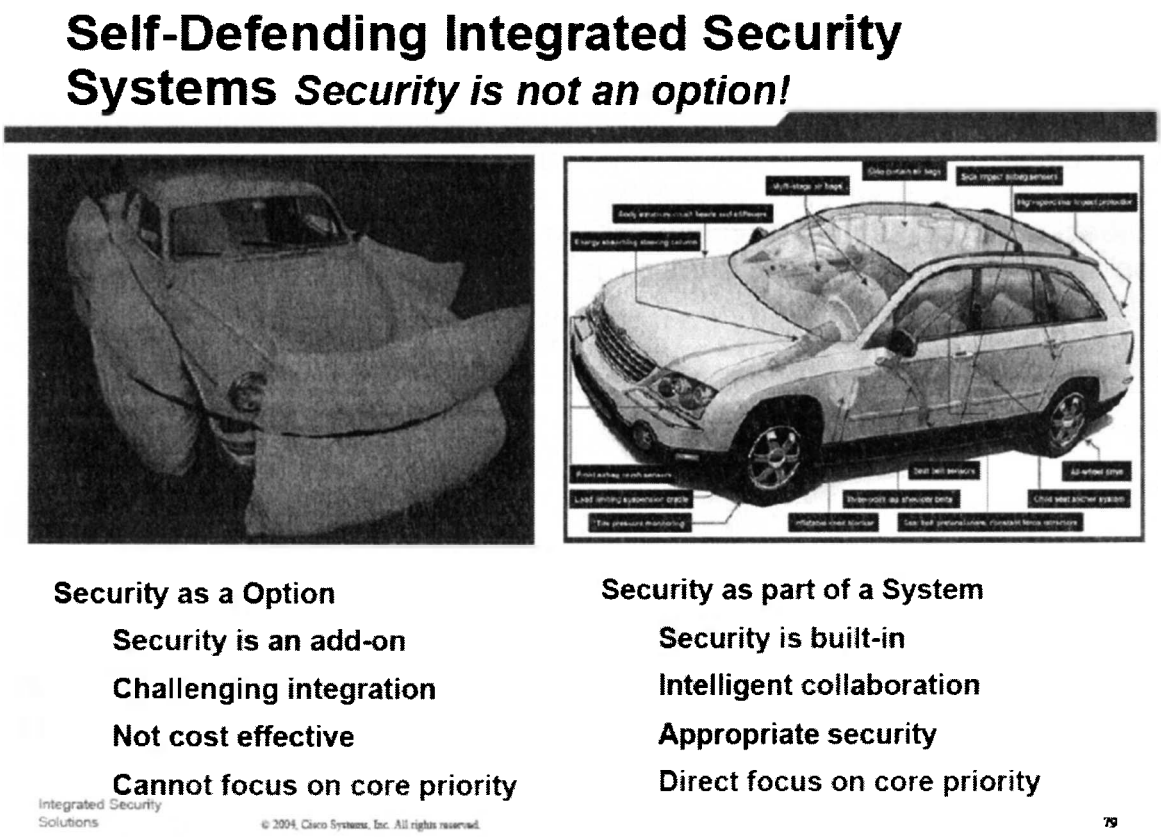


Figura 3.2 Concepción de algunos gerentes sobre la seguridad informática.

El pensamiento anterior, se puede atribuir a que los actuales gerentes crecieron en las empresas cuando los incidentes de seguridad eran mínimos o cuando las tecnologías de información (TI) no eran crucial para las operaciones de la empresa.

La revista por Internet universia.net.mx comenta en el 2004, que la mayoría de los directores o consejos directivos de una empresa reciben cada año, o casi nunca, un informe sobre la seguridad de su información, de acuerdo con una encuesta realizada por la firma Mancera Ernst & Young. La misma revista comenta, que alrededor de un 56% de los directivos mundiales encuestados señalaron que se reúnen muy pocas veces o casi nunca con su área de seguridad de la información. En México fueron alrededor de 60 empresas las que contestaron el cuestionario, el total fueron mil 230 compañías de 51 países.

3.2 Trabajo del diseño de una política de seguridad

Después de poder involucrar a todo el personal técnico y gerencial se necesita proseguir con la creación de la política de seguridad de la empresa; la cual iniciará con una planeación y posteriormente con el diseño, implementación, operación y operación. Al concluir la operación de este ciclo; se tendrá que evaluar, redefinir e iniciar una nueva política acorde a las nuevas necesidades de seguridad (Cisco System, 2004). La figura 3.3 ejemplifica este ciclo de trabajo.

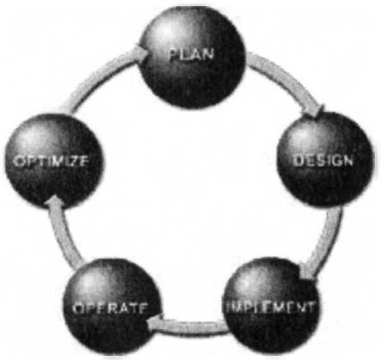


Figura 3.3 Proceso de trabajo en una política de seguridad.

La Política de Seguridad tiene dos propósitos centrales: Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de Información y ofrecer las guías para actuar ante posibles amenazas y problemas presentados (Universidad Nacional de Colombia. 2004).

Por otro lado, la política se debe basar en el análisis de riesgo y tener como objetivo la estandarización de entornos y procesos de manera que se eviten las vulnerabilidades existentes. Su creación está directamente conectada a la concretización de este análisis, pues a través del levantamiento de las vulnerabilidades se puede elaborar la documentación de seguridad, con el objetivo de minimizar los riesgos de que las amenazas se conviertan en incidentes (Academia Latinoamericana de Seguridad Informática, 2004).

Es importante recalcar que no se puede eliminar el riesgo, sólo se gestiona o administra (CA Computer Associates, 2004).

La clasificación del riesgo se contemplará en bajo, mediano y alto (Cisco System. 2005) y se pretende sea acorde con los activos importantes de la empresa. No se pretende caer en el concepto de que todo es crítico para la empresa; dado que ha mayor seguridad el incremento en los costos para lograr la misma serán considerables. La figura 3.4 ejemplifica el concepto de gestión de la seguridad y cómo existe una inflexión de toma de decisión en la cual existe un grado máximo de seguridad aún cuando se siga invirtiendo en ella (Gordon, 2003)

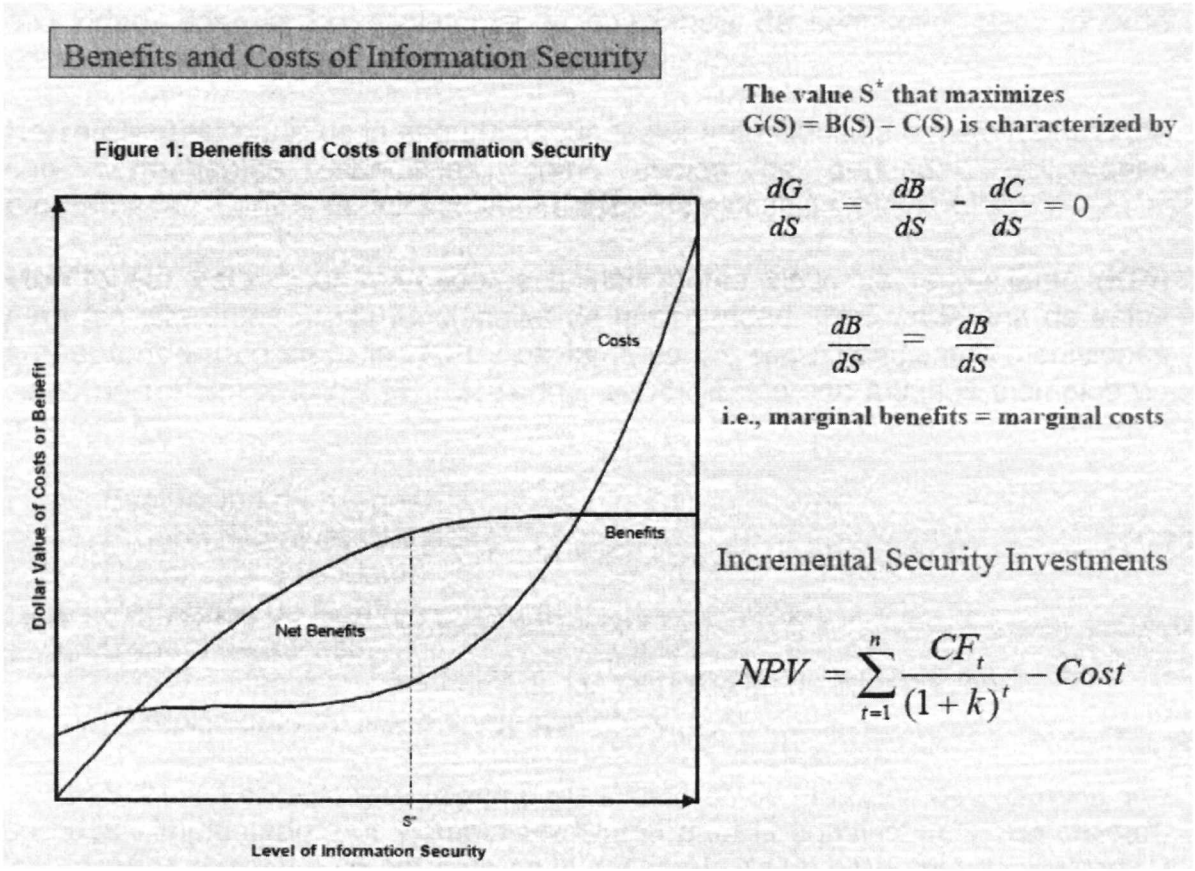


Figura 3.4 Relación costo beneficio de la seguridad computacional.
Fuente: University of Maryland Institute For Advanced Computer Studies

Complementando lo anterior, se considera que además el ser humano puede ser un factor de riesgo importante por su ingenuidad o negligencia. Encuestas y estudios CSI, Gartner, E&Y, PwC, Information Week, US GAO, etc. reafirman la conclusión que las amenazas están aumentando y que existen problemas importantes en la misma operación de la organización.

3. 3 Implementación de la política de seguridad ¿cómo iniciar?

Un buen inicio es contar con los siguientes elementos como base de sustentación: Cultura, Herramientas y Monitoreo (Academia Latinoamericana de Seguridad Informática, 2004). Definiendo cada uno de ellos encontramos:

Cultura: el entrenamiento de personas debe ser constante, de tal manera que se actualice toda la empresa con relación a los conceptos y normas de seguridad, además de sedimentar la conciencia de seguridad, para tornarla como un esfuerzo común entre todos los involucrados.

Herramientas: parte de la seguridad puede ser automatizada o mejor controlada con herramientas específicas, como copias de seguridad obligatorias programadas, control de acceso con registro de ejecución, etc.

Monitoreo: establecer marcadores e indicadores clave de rendimiento (KPI) para las diferentes áreas funcionales de la seguridad. Para cada una de estas áreas, tendrá que crear los KPI y obviamente las correspondientes mediciones clave de rendimiento (KPM) (McCarthy, 2004). Estos son algunos ejemplos de métricas:

- Evaluación de riesgos.
- Prueba de vulnerabilidades.
- Respuesta a incidente.
- Protección de la infraestructura.
- Control de acceso.
- Entrenamiento en seguridad de las tecnologías de información.
- Cumplimiento de las reglamentaciones.

Si busca en su organización otras iniciativas de medición de procesos que se hayan implantado, por ejemplo Six Sigma para la administración de calidad, los desafíos a los que se enfrenta en el desarrollo de un programa de métricas y mediciones de seguridad no serán muy diferentes a aquéllos que surgen cuando se adopta un sistema de administración de calidad total (TQM) (McCarthy, 2004)

Otro punto a considerar, es tener en cuenta lo que preocupa a los gerentes y que se relaciona con la seguridad informática (ebusinessforum Grecia, 2004)

- Costos en dólares de downtime (tiempos de inactividad de los sistemas).
- La facilidad en que al ser vulnerables se pierde ventajas competitivas.
- La competencia presenta ventajas en proveer mayor disponibilidad de servicios.
- La compañía es inmune a vulnerabilidades.
- Impactos en el negocio principal (core-business) de la empresa.

Para el caso de las universidades se puede citar la entrevista en el agosto del 2004 con Juan José Zamanillo consultor de la Vicerrectoria de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM). El comenta que se cuida el negocio principal (core-business) de la empresa como son las videoconferencias y las plataformas tecnológicas. Nosotros vendemos educación con tecnología por lo cual estás deben de estar siempre operacionales.

Por último, es trabajar con base a estándares de seguridad y de buenas prácticas. Las normas de British Standards Institute (BSI) e Internacional Organization for Standardization (ISO) son un paso importante.

3.3.1 Normas ISO 17799, BS 7799-1 y BS 7799-2

La ISO 17799 es una guía de buenas prácticas de seguridad informática que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de las tecnologías de información sino que hace una aproximación holística a la seguridad de la información abarcando todas las funcionalidades de una organización en cuanto a que puedan ser afectadas por la seguridad informática. La ISO 17799 sólo hace recomendaciones sobre el uso de controles de seguridad. No establece requisitos cuyo cumplimiento pudiere certificarse (unixmexico, 2004)

Haciendo referencia a las páginas electrónicas
http://www.iso-17799-security-world.co.uk/def.htm y
http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm se comentan las diez rúbricas que toma la norma 17799

Políticas de seguridad. El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

Seguridad organizacional. Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de entrega de servicios especializados a un tercero (outsourcing), entre otros aspectos.

Clasificación y control de activos. El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

Seguridad del personal. Contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.
El objetivo de esta área del estándar es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

Seguridad física y de entorno. Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

Comunicaciones y administración de operaciones. Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

Control de acceso. Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

Desarrollo de sistemas y mantenimiento. La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

Continuidad de las operaciones de la organización. El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

Requerimientos legales. La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.
Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

La ISO 17799 es prácticamente igual a la Primera Parte de la norma BS 7799; la BS 7799-1. Esta norma británica tiene una Segunda Parte, BS 7799-2, que usa la expresión verbal "must", otro término habitual en ciertas normas para expresar mandato u obligación. Los requisitos que se especifican de esta manera se refieren a un Plan de Seguridad constituido por un Sistema de Gestión de Seguridad Informática (SGSI), en el que se aplican los controles de seguridad de la BS 7799-1 (y por lo tanto de la ISO 17799). Los requisitos que se establecen en el SGSI de la BS 7799-2 se pueden auditar y certificar. No hay versión ISO de la BS 7799-2 (unixmexico, 2004).

La flexibilidad e imprecisión de ISO 17999 es intencional por cuanto es difícil contar con una norma que funcione en una variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 177999 simplemente ofrece un conjunto de reglas a un sector donde no existían (Symantec, 2003).

Un buen trabajo constaría de complementar la ISO 17999 con la BS 7799-2 para un entorno completo de política de seguridad, teniendo así mayores bases de una política de seguridad robusta y aplicable para cualquier organización pequeña o grande o en nuestro caso universidades. Un ejemplo en México es la UNAM (Universidad Nacional Autónoma de México) (Núñez, 2005).

En Estados Unidos la Universidad de California BerKeley cuenta con su política de seguridad y se muestra en la tabla 3.1

- Introduction
- Policy
- Roles and Responsibilities
- Key Security Elements
- Privacy and Confidentiality
- Compliance with Law and Policy
- Resources

Tabla 3.1 Contenido de la política de seguridad de la Universidad de California BerKeley

3.4 Factores de éxito de una política de seguridad

Un reto importante para el éxito de una política de seguridad, es lograr todo lo anterior emitiendo un documento sencillo y claro, apoyado por la alta dirección, que permita la normal actuación, haciendo de las políticas procedimientos inmersos en los tareas cotidianas, enfocados a los problemas relevantes, fácil de ajustar a los cambios permanentes, que garanticen su cumplimiento apoyándose en herramientas de seguridad antes que orientado a castigar a los infractores, lo cual no se descarta. Pero hay que resaltar algunas características que hacen de ella una buena Política de Seguridad: La constante actualización y el hacerla pública y respaldada por los usuarios en la vida práctica (Universidad Nacional de Colombia. 2004).

Adicionalmente hay que comentar que cuando sucedan casos de sanciones deberán ser aplicados. La Universidad de California BerKeley comenta lo siguiente: la insuficiencia de medidas en cualquier nivel puede causar que las fuentes sean demandada, robadas o empezar ser un problema en el campus. La responsabilidad y acciones deben de ser tomadas. Por ejemplo, en una situación de demanda de recursos con por una computadora será bloqueada en su acceso a red.

El director de CETI UC Marcos Sepúlveda en la revista Gerencia de Costa Rica (2003) comenta como lo muestra la figura 3.5 los puntos a cuidar cuando se implementa una política de seguridad.

Fuente: Desayuno Club CIO, Noviembre 2004

Figura 3.5 Principales obstáculos para una buena seguridad.

3.5 Relación de la política de seguridad con el método propuesto de investigación

Al plantear la normatividad adecuada para el desempeño de la seguridad computacional es necesario entonces relacionar la importancia de apoyo al método de estudio.

Una política de seguridad apoya directamente los puntos el método que son:

1) **Análisis de riegos**: Con base a una relación de riesgo de los virus gusano, el inventario de activos deberá ser administrado y controlado de acuerdo a su nivel de confidencialidad e impacto a la institución educativa.
2) **Plan de acción:** Amparo de las acciones con las directrices de seguridad de la institución educativa.
3) **Implementación de las soluciones:** Al definir un proyecto, un responsable, tiempos y participaciones de las áreas involucradas, la política de seguridad apoya a la implementación y al cuidado de controles obligatorios para toda organización y para los proveedores, socios y usuarios formalizados en los contratos o convenios.
4) **Operación de las soluciones**: Estatutos de la operación de las medidas de seguridad cuidando los controles a las acciones del personal que opera con los activos de información. Continuidad de las operaciones de la organización.
5) **Mantener las soluciones**: Desarrollo de sistemas y mantenimiento.

Capítulo 4

Metodología de investigación

La metodología de investigación que se utilizó durante el desarrollo de la tesis fue cuantitativa. Existe una deducción donde inicialmente se tiene una teoría y se trata de probar que tan válido y aplicable es el método que se propone. Se trabajó con un modelo particular con un estudio de cinco variables para explorar el conocimiento, la cuantificación, el tratamiento, las acciones y las mejoras de éstas, para disminuir la amenaza de los virus gusano (worms) en las universidades de México.

4.1 Modelo particular

La figura 4.1 muestra el modelo particular de esta investigación, donde se contempla las cinco variables interesantes al método propuesto.

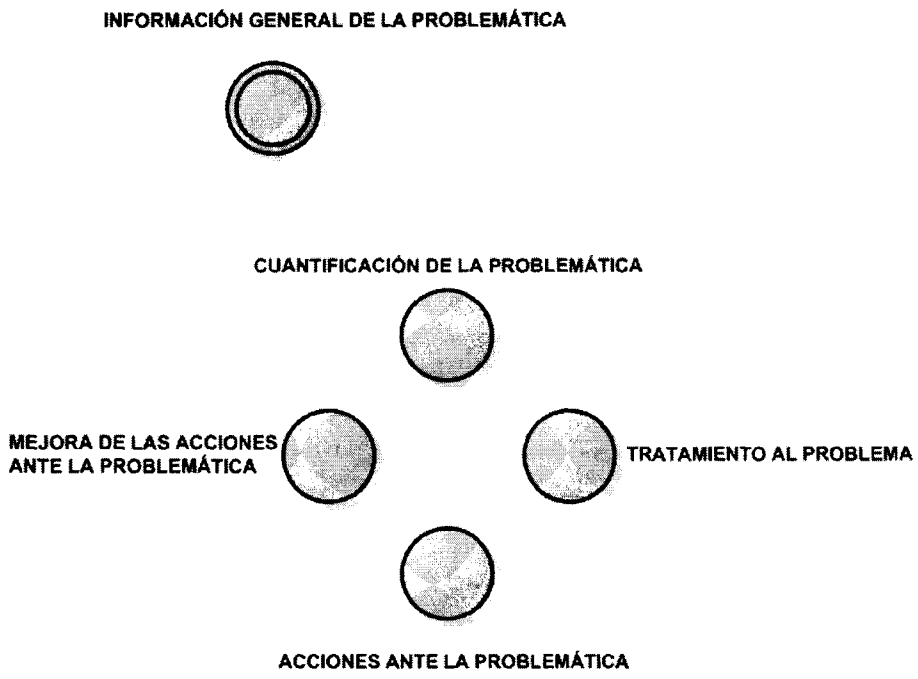


Figura 4.1 Modelo particular de estudio.

4.2 Especificación de las variables

1. **Información de la problemática**: pretende sondear al grado de impacto en las universidades de México ante los virus gusano (worms). Adicionalmente se pretende conocer las fuentes identificadas de la amenaza y las áreas de oportunidad que la universidad detecta importantes en su infraestructura cuando hay problemas de virus gusano (worms).
2. **Cuantificación de la problemática:** pretende obtener si se realiza o no una medición de cuántos virus gusano (worms) existen en la institución educativa y la proporción de tráfico que genera éstos. Si se desarrolla la medición, se indaga del porcentaje de participación de los virus gusano en los rubros de cantidad de máquinas con virus y tráfico. Adicionalmente se contempla cuanto tiempo le cuesta a un trabajador remover un virus gusano (worm) de una máquina.
3. **Tratamiento del problema:** sondeo de las soluciones técnicas y de negocio ante la amenaza de virus gusano (worms). Se indaga en la profundidad y aplicación de los análisis de seguridad y de viabilidad económica.
4. **Acciones ante la problemática:** sondeo de las soluciones realizadas para minimizar el riesgo de virus gusano (worm). Se contempla soluciones comerciales y de código abierto, la estrategia realizada (si es reactiva o preactiva) y el análisis de viabilidad económica que implica implementar dichas soluciones.
5. **Mejora de las acciones ante la problemática**: variable de mejora que implica la existencia de retroalimentación de las variables anteriores.

4. 3 Método de estudio

Cuantitativa

- **Encuestas:** se realizó un estudio de sondeo que pretendió ubicar las actividades, conocimiento y estrategias que el personal administrativo y técnico realiza en las universidades de México, para mitigar el impacto de los virus gusano (worms). La encuesta apoya directamente al método propuesto en este estudio de tesis.

4. 4 Población

La población para esta investigación, consta de las universidades que tienen la infraestructura de Internet 2 contempladas en la página de la Corporación Universitaria para el desarrollo de Internet A. C. (cudi) cuya dirección electrónica es http://www.cudi.edu.mx/

Específicamente se selecciona 33 afiliados académicos y los 20 asociados académicos, contemplando únicamente un campus o sede en las universidades que tienen mas de un punto de presencia, salvo el caso del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) el cual se realiza un estudio completo de todos sus campus.

Las personas encuestadas tienen la facultad de ofrecer información relevante propia de sus institución ya sea técnica o directiva y se contempló una persona por universidad y por el lado del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) 1 ó 2 por campus. La decisión anterior es por la disponibilidad, confidencialidad y acceso a las universidades.

Al tener toda la población del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) se tiene un censo que puede no ser la situación global de todas las universidades de México, pero la investigación contempla el contraste con las demás universidades de México.

El universo de estudio fue entonces 53 universidades.

Dado que el universo es finito el cálculo de encuesta se realiza de la siguiente manera:

$$n = \frac{Z^2 P(1-P)N}{e^2(N-1) + Z^2 P(1-P)}$$

donde:
n=tamaño de la muestra;
Z= nivel de confiabilidad, generalmente se usa 95%;
P=probabilidad de éxito de que las personas que se seleccionan tengan las características que se requieren. Dado que se realizó un estudio previo para recolectar a las personas indicadas que contienen características directivas o técnicas y que además ofrecen información objetiva de la totalidad de la institución donde laborar se considera que 9 de cada 10 personas es confiable.
e= error esperado. Se consideró un 5% de error.
N= tamaño de la población; el cual es de 53 universidades.
Al aplicar los cálculos nos considera 20.38 encuestas las cuales se cerró 21 encuestas.

Capítulo 5

Resultados de las encuestas

En este capítulo se darán a conocer los resultados obtenidos en las encuestas aplicadas al grupo muestra seleccionado, así como también se mostrará el análisis de dichos resultados para generar las conclusiones de este estudio.

5.1 Descripción

El estudio considera la hipótesis de que los virus gusano al propagarse en la red de una universidad, impactan económicamente a la organización y reducen la productividad de las actividades en una computadora.

5.2 Realización

La encuesta fue realizada en una base de datos con lotus y ligada a una página de web cuya dirección electrónica fue:
http://rzprzph1.gda.itesm.mx/utils/ramiro/encuesta.nsf/introduccion?OpenForm
y su estructura se lista en el anexo A al final de este estudio.

5.3 Estrategia de recolección de datos

Se mandó correos electrónicos a las personas seleccionadas en la base de datos del CUDI y además por cuestiones de disponibilidad se realizó vía telefónica a varias personas este cuestionario.

5.4 Análisis de resultados

El la tabla 5.1 se muestran las preguntas realizadas en la encuesta en relación con las variables interesantes del estudio y que apoyan al método propuesto.

Variables del estudio	**Preguntas**
Información general de la problemática	1,2 y 3
Cuantificación del problema	4, 5, 6, 7 y 8
	9, 10, 11, 12, 13, 14, 15, 16 y
Tratamiento del problèma	17
Acciones ante la problemática	18, 19, 20, 21 y 22
Mejora de las acciones ante la problemática	23 y 24

Tabla 5.1 Relación de preguntas y variables de estudio.

5.5 Clasificación de datos

El estudio será clasificado en tres secciones, para poder contrastar los resultados. Con base al tamaño de campus del ITESM, serán clasificados en grandes (Monterrey, Edo de México, Ciudad de México, Toluca, Guadalajara y Querétaro) y medianos-chicos (los demás campis del sistema ITESM; consultar su página electrónica en www.itesm.mx). Se toma como tercera sección las otras universidades. Una nota importante para el estudio es considerar que el ITESM tiene un modelo centrado en el alumno y con una infraestructura tecnológica que lo sustenta desde hace varios años. Otras universidades de México como la UNAM y UDG incursionan en una estrategia similar en fechas recientes.

Por razones de confidencialidad y por la opción de poner o no la información de la universidad encuestada no se diferencia entre universidades; se mandaron 50 encuestas y se contestaron 21 cumpliendo que fueran universidades miembros del CUDI.

La nomenclatura usada es: Universidades de México (CUDI), Campis medianos y chicos del ITESM (ITESM2) y Campis grandes del ITESM (ITESM).

5. 6 Trabajo de la variable uno "información general de la problemática"

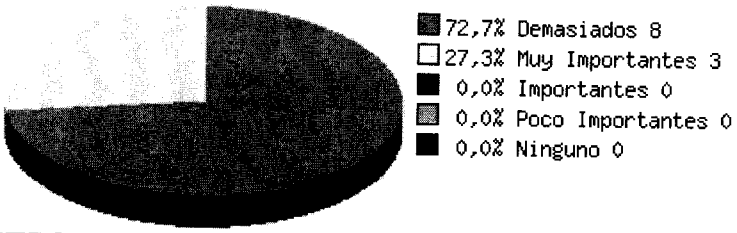
La tabla 5.2 relaciona las tres preguntas de la variable "información general de la problemática" con la frecuencia mas importante en cada sección de estudio.

Información general de la problemática	CUDI	ITESM2	ITESM
Magnitud	[redacted]	Importantes	[redacted]
Afectación principal del problema	Saturación de enlaces y corrupción de datos de cómputo.	Saturación de enlaces, impresión y comunicación con plataformas tecnológicas.	Todas las opciones.
Adquisición del problema	Ejecución de archivos contaminados.	Adquisición en red por vulnerabilidades en el sistema operativo.	Adquisición en red por vulnerabilidades en el sistema operativo.

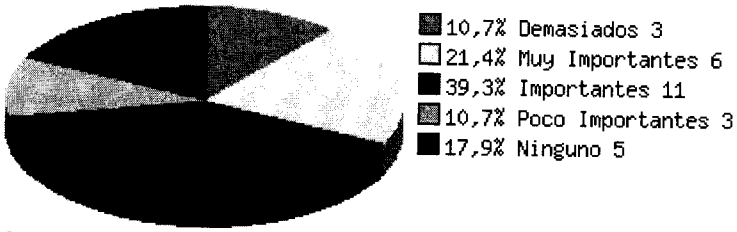
Tabla 5.2 Relación de comparación de la variable "información general de la problemática" en tres segmentos de estudio.

La figura 5.1 representa el panorama general de los tres segmentos y la concepción de técnicos y directores sobre el problema en general de los virus gusano (worms).

ITESM



ITESM2



CUDI

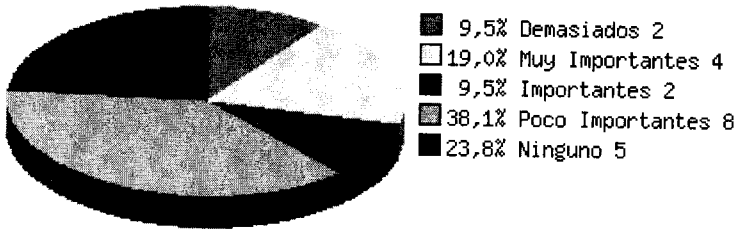
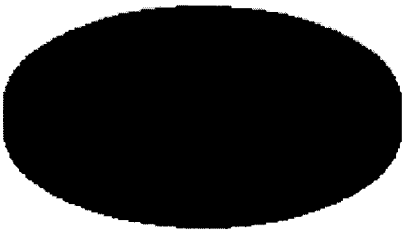


Figura 5.1 Concepción general de la problemática sobre virus gusano (worms).

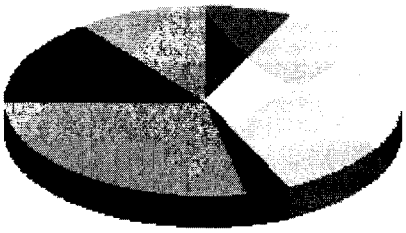
En la figura 5.2 encontramos cuales son los factores de impacto más comunes en las universidades de México con respecto a los virus gusano (worms).

ITESM



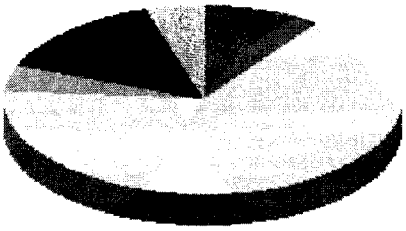
0,0% Comunicación con las plataformas tecnológicas 0
0,0% Impresión por red 0
0,0% Voz sobre Ip (VOIP),Telefonía IP y servicios sensibles al retraso 0
0,0% Denegación de servicio (DOS) 0
0,0% Saturación de enlaces 0
0,0% Corrupción de datos en equipo de cómputo 0
0,0% Baja productividad en el personal debido a remover los virus 0
100,0% Todas las respuestas aplican. 11

ITESM2



7,1% Comunicación con las plataformas tecnológicas 2
35,7% Impresión por red 10
3,6% Voz sobre Ip (VOIP),Telefonía IP y servicios sensibles al retraso 1
28,6% Denegación de servicio (DOS) 8
10,7% Saturación de enlaces 3
3,6% Corrupción de datos en equipo de cómputo 1
10,7% Baja productividad en el personal debido a remover los virus 3
0,0% Todas las respuestas aplican. 0

CUDI

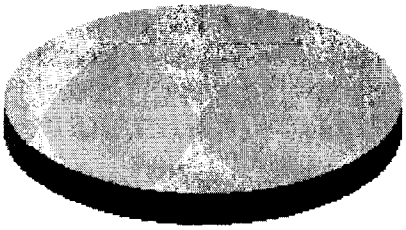


9,5% Comunicación con las plataformas tecnológicas 2
66,7% Impresión por red 14
0,0% Voz sobre Ip (VOIP),Telefonía IP y servicios sensibles al retraso 0
4,8% Denegación de servicio (DOS) 1
4,8% Saturación de enlaces 1
9,5% Corrupción de datos en equipo de cómputo 2
4,8% Baja productividad en el personal debido a remover los virus 1
0,0% Todas las respuestas aplican. 0

Figura 5.2 Concepción general del impacto de los virus gusano (worms).

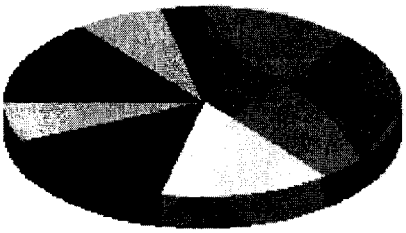
Para concluir la variable uno que nos ofrece la información general de la problemática, se contempla el panorama de adquisición de virus gusano (worms) en las universidades de México en la figura 5.3

ITESM



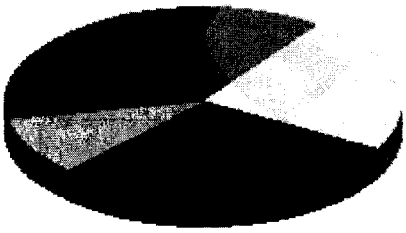
- 0,0% Adquisición en red. 0
- 0,0% Ejecución de archivos contaminados. 0
- 0,0% Archivos anexos por correo (mail). 0
- 0,0% Aceptación de archivos por mensajería instantánea. 0
- 0,0% Vulnerabilidades en la visualización de .jpg 0
- 0,0% Uso de programas p2p (peer-to peer). 0
- 100,0% Todas las anteriores respuestas suceden. 11
- 0,0% No conozco ninguna que suceda. 0

ITESM2



- 39,3% Adquisición en red. 11
- 14,3% Ejecución de archivos contaminados. 4
- 14,3% Archivos anexos por correo (mail). 4
- 7,1% Aceptación de archivos por mensajería instantánea. 2
- 0,0% Vulnerabilidades en la visualización de .jpg 0
- 14,3% Uso de programas p2p (peer-to peer). 4
- 7,1% Todas las anteriores respuestas suceden. 2
- 3,6% No conozco ninguna que suceda. 1

CUDI



- 9,5% Adquisición en red. 2
- 23,8% Ejecución de archivos contaminados. 5
- 28,6% Archivos anexos por correo (mail). 6
- 9,5% Aceptación de archivos por mensajería instantánea. 2
- 4,8% Vulnerabilidades en la visualización de .jpg 1
- 4,8% Uso de programas p2p (peer-to peer). 1
- 0,0% Todas las anteriores respuestas suceden. 0
- 19,0% No conozco ninguna que suceda. 4

Figura 5.3 Concepción general de las fuentes de adquisición de virus gusano (worms).

5.7 Trabajo de la variable dos "cuantificación del problema"

Para el estudio de esta variable se contempla en primer instancia; si se realiza o no una medición del problema y si es realizada esta medición que porcentaje implica en la población de máquinas, recursos de salida (enlaces) y tiempo de reparación de máquina con problemas debidos a los virus gusano (worms). La tabla 5.3 contempla el resumen de los datos obtenidos en una clasificación acorde a lo planteado en la distribución de población encuestada.

Cuantificación del problema	CUDI	ITESM2	ITESM
Medición de máquinas vulnerables	-No se contestó la pregunta -Si se contestó predominó el NO	-No se contestó la pregunta -Si se contestó predominó el NO	-No se contestó la pregunta -Si se contestó predominó el NO
Cuantificación de máquinas vulnerables	-Generalmente no se sabe. - Comprende un rango del 20% al 50%.	-Generalmente no se sabe. - Comprende un rango del 20% al 50%.	-Generalmente no se sabe. - Comprende un rango del 20% al 50%.
Medición de tráfico en enlaces	Prevalece el SI, sin embargo existen muchos NO	SI	SI
Cuantificación de tráfico en enlaces	10%	20% al 50%	20% al 50%
Tiempo en reparación de máquinas	1 hora	1 hora	1 hora

Tabla 5.3 Relación de comparación de la variable "cuantificación del problema" en tres segmentos de estudio.

5.7.1 Anotaciones importantes de esta variable

Las personas que contestaron a las preguntas se encuentran los siguientes patrones:

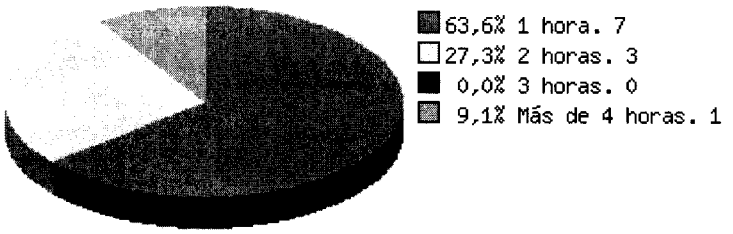
a) Si existe un dato de cuantificación, éste es realizado por personal técnico y generalmente esa información la desconocen sus superiores (directores).
b) En los tres grupos se concluye que se desconoce el número de máquinas vulnerables aún cuando en la pregunta 6 exista (al parecer) una concepción de que se encuentran entre el 20% y 50% de

máquinas vulnerables de la población total de máquinas en la institución educativa.

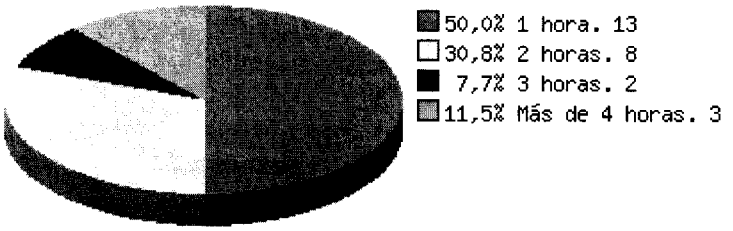
c) La pregunta de cuánto tiempo en general se lleva para reparar una máquina dañada por virus gusano (worms) predomina la respuesta de 1 hora, sin embargo; en específico del ITESM, en el grupo de encuestados se encuentra personas que tienen más contacto con clientes y sobre todo sensible al conocimiento de cuánto le cuesta, a ellos y a su personal a cargo, el reparar máquinas y en promedio se encuentra su respuesta en 2 horas.

La figura 5.4 relaciona el tiempo de reparación de máquinas en los diferentes grupos de estudio.

ITESM



ITESM2



CUDI

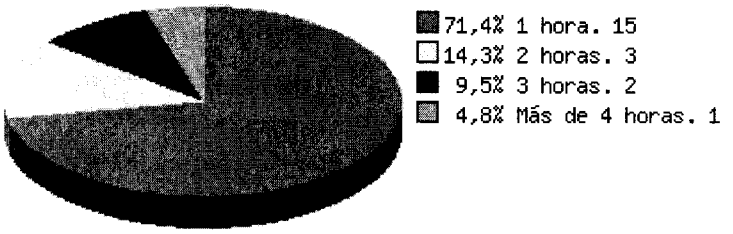


Figura 5.4 Concepción general del tiempo de reparación de máquinas con virus gusano (worms).

5.8 Trabajo de la variable tres "tratamiento del problema"

El tratamiento del problema, contempla un estudio estructurado del riesgo de los virus gusano (worms) con su impacto al negocio. Se prendió sondear y numerar los factores importantes de seguridad y negocio en las universidades de México. Esta es la variable, que dispara el estudio y la contrasta entre una universidad y una empresa privada. Ver la tabla 5.4 que representa las respuestas más frecuentes de las universidades de México.

Tratamiento del problema	CUDI	ITESM2	ITESM
Tiene reuniones de seguridad informática	De 1 a 5 veces al año.	De 1 a 5 veces al año.	De 1 a 5 veces al año.
Realiza un análisis de riesgo.	NO	NO	NO
Factores importantes en un análisis de riesgo.	-Contempla dispositivos vulnerables y fuentes de riesgos. -Frecuencia y probabilidad de aparición de virus gusano (worms).	-Contempla dispositivos vulnerables y fuentes de riesgos. -Frecuencia y probabilidad de aparición de virus gusano (worms).	Todas las anteriores.
Cuenta con una política de seguridad	NO	NO	NO
Alcance de los estatutos de la política de seguridad	Ninguno	Ninguno	Ninguno
Realiza un análisis de costos de productividad	NO	NO	NO
Factores importantes en un análisis de productividad.	-Relación tiempo/costo de técnicos en reparar equipo. -Pérdida de información. -Imagen de la institución	-Relación tiempo/costo de técnicos en reparar equipo. -Pérdida de información. -Relación tiempo/productividad	-Todas las respuestas.

	educativa.	por no realizar actividades.	
Realiza un análisis de costos de oportunidad.	NO	NO	NO
Factores importantes en un análisis de oportunidad.	Todas las respuestas aplican.	Disponibilidad de recursos que pudiera impedir una entrada económica a la institución educativa. Por ejemplo, si se ofrece un diplomado y el sistema de tesorería no se encuentra disponible, ocasiona que se pierda un ingreso de colegiatura de un aspirante a este diplomado.	Todas las respuestas aplican.

Tabla 5.4 Relación de comparación de la variable "tratamiento del problema" en tres segmentos de estudio.

5.8.1 Anotaciones importantes de esta variable

a) Lo que para una empresa bancaria o que depende de sus sistemas de información es una frecuente actividad; el estudio revela que no lo es para las universidades de México.
b) Resalta cómo las teorías estructuradas de seguridad y lo que la consultoría realiza en los análisis propuestos no se realiza en las universidades de México; aún cuando presentan conocimiento de cuales son los factores a considerar en éstos.
c) Existe mayor conciencia en "la imagen de la institución" por parte de las universidades encuestadas del cudi que por los campis del ITESM; sin embargo, se contempla en todas las respuestas anteriores que es la opción total en el segmento de ITESM que son los campis grandes.
d) Lo que para las empresas, las estrategias de negocio, las buenas enseñanzas de un posgrado de administración comentan como "impacto al negocio", "criticidad de los activos" y "disponibilidad" son ausentes en las universidades de México.
e) El segmento ITESM2, que son los campis de mejor tamaño del sistema ITESM, cuentan con una concepción importante en el análisis de costos

de oportunidad. Estos campis, en que una fuente de ingresos importantes son los diplomados, tienen más claro este impacto a comparación de los campis grandes.

5.9 Trabajo de la variable cuatro "acciones ante la problemática"

La variable cuatro, tiene que ver directamente en la actitud del problema. El comportamiento reactivo, preventivo y la concepción de cuánto cuesta implementar la tecnología usada. Se verifica además cómo se implementa; es decir, al implementar, operar y mantener las actividades para minimizar los virus gusano (worms) se ¿contempla personas, procedimientos y tecnología?. La tabla 5.5 nos presenta el resultado de estos cuestionamientos.

Acciones ante la problemática	CUDI	ITESM2	ITESM
Comportamiento	Reactivo/preventivo	Reactivo/preventivo	Reactivo/preventivo
Actividades para minimizar los worms.	Cuestionable el resultado→ Se selecciona cada respuesta en todos los encuestados.	-Instalación de un firewall. -Bloqueo de máquinas generadoras de tráfico dañino. -Instalación de un antivirus en máquinas. -Actualización del sistema operativo. -Campañas de educación. -Segmentación lógica de la red (vlans).	-Instalación de un firewall. -Bloqueo de máquinas generadoras de tráfico dañino. -Instalación de un antivirus en máquinas. -Actualización del sistema operativo. -Campañas de educación. -Segmentación lógica de la red (vlans). -Uso de herramientas open source (código abierto) para detectar máquinas vulnerables. -Acceso controlado de máquinas a la

			red (registro de red).
Realiza un estudio de viabilidad económica.	SI	SI	SI
Elementos de su estudio de viabilidad económica.	ROI	ROI	ROI
Al implementar, operar y mantener sus actividades para minimizar los virus gusano (worms) ¿contempla personas, procedimientos y tecnología?	SI	SI	SI

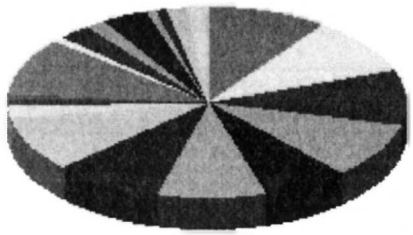
Tabla 5.5 Relación de comparación de la variable "acciones ante la problemática" en tres segmentos de estudio.

5. 9.1 Anotaciones importantes de esta variable

a. Los encuestados en general, afirman usar el análisis ROI para su viabilidad económica.
b. Las 21 encuestas realizadas a personal de las universidades del CUDI contestan las 22 opciones de soluciones para minimizar el impacto ante los virus gusano (worms). Esta pregunta en particular hace pensar dos casos:
    i. Las universidades de México, que no tienen la misma infraestructura del ITESM, algunas incursionan hace poco años atrás con videoconferencias y con modelos de educación a distancia y que en el panorama general comentan que los virus gusanos (worms) es un problema poco importante ¿realizan todas las soluciones?
    ii. El personal que realizó las encuestas (CUDI) asume que el poner todas las soluciones ¿no evidenciará su capacidad tecnológica en general?
    iii. El personal que realizó las encuestas (CUDI) asume que exponer que hacen o no en específico es poner en la mesa sus debilidades tecnológicas y ¿realizaron una estrategia de no exponer sus vulnerabilidades?
c. Para efectos del estudio esta variable no será comparada con los otros dos segmentos, ITESM e ITESM2.

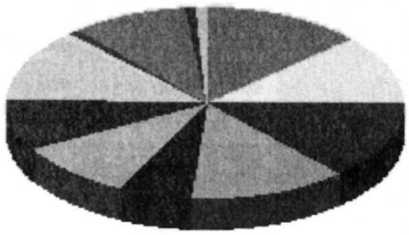
La figura 5.5 contempla las acciones realizadas en el ITESM en general para minimizar la amenaza de los virus gusano (worms). Se descarta al grupo CUDI dado que en las 21 encuestas realizadas, las personas de estas universidades contestaros las 22 opciones.

ITESM



- 9,6% Instalación de un firewall. 11
- 9,6% Bloqueo de máquinas generadoras de tráfico dañino. 11
- 9,6% Instalación de un antivirus en máquinas. 11
- 9,6% Actualización del sistema operativo. 11
- 4,3% Actualización de paquetería Office de Microsoft. 5
- 2,6% Configuraciones en clientes de correo para combatir worms. 3
- 8,7% Instalación de software antispyware. 10
- 8,7% Campañas de educación. 10
- 9,6% Sigo la recomendación del 1,2,3 de Microsoft. 11
- 1,7% Sigo la recomendación del 1-12 de Trend (compañía de antivirus). 2
- 1,7% Integración de máquinas a un dominio de Microsoft y SUS. 2
- 0,9% Integración de herramientas como NAC y CSA. 1
- 9,6% Segmentación lógica de la red (vlans). 11
- 0,9% Uso de tecnología 802.1x 1
- 2,6% Uso de herramientas open source para detectar máquinas vulnerables. 3
- 1,7% Uso de tecnología IDS. 2
- 1,7% Uso de tecnología IPS. 2
- 1,7% Correlación de alarmas entre herramientas de monitoreo, IDS e IPS. 2
- 0,9% Uso de tecnología de vlans dinámicas. 1
- 0,9% Uso de tecnología Private VLANs. 1
- 1,7% Acceso controlado de máquinas a la red (registro de red). 2
- 1,7% Monitoreo de peticiones de nombre por máquina al DNS. 2

ITESM2



- 13,0% Instalación de un firewall. 28
- 12,1% Bloqueo de máquinas generadoras de tráfico dañino. 26
- 13,0% Instalación de un antivirus en máquinas. 28
- 13,0% Actualización del sistema operativo. 28
- 4,7% Actualización de paquetería Office de Microsoft. 10
- 1,4% Configuraciones en clientes de correo para combatir worms. 3
- 9,3% Instalación de software antispyware. 20
- 9,3% Campañas de educación. 20
- 11,2% Sigo la recomendación del 1,2,3 de Microsoft. 24
- 0,9% Sigo la recomendación del 1-12 de Trend (compañía de antivirus). 2
- 0,9% Integración de máquinas a un dominio de Microsoft y SUS. 2
- 0,0% Integración de herramientas como NAC y CSA. 0
- 9,3% Segmentación lógica de la red (vlans). 20
- 0,0% Uso de tecnología 802.1x 0
- 0,9% Uso de herramientas open source para detectar máquinas vulnerables. 2
- 0,0% Uso de tecnología IDS. 0
- 0,0% Uso de tecnología IPS. 0
- 0,0% Correlación de alarmas entre herramientas de monitoreo, IDS e IPS. 0
- 0,0% Uso de tecnología de vlans dinámicas. 0
- 0,0% Uso de tecnología Private VLANs. 0
- 0,9% Acceso controlado de máquinas a la red (registro de red). 2
- 0,0% Monitoreo de peticiones de nombre por máquina al DNS. 0

Figura 5.5 Actividades que se realizan en el ITESM en general para minimizar la amenaza de virus gusano (worms).

5.10 Trabajo de la variable cinco "mejoras de las acciones ante la problemática"

A un ciclo de acciones, es recomendable retroalimentar y fomentar la mejora de las estrategias y acciones realizadas. La tabla 5.6 representa lo que no se realiza en las universidades de México.

Acciones ante la problemática	CUDI	ITESM2	ITESM
¿Realiza un estudio de costo-beneficio de las soluciones y actividades para evaluar objetivamente si el esfuerzo vale la pena?	NO	NO	NO
¿Existe un ciclo de retroalimentación, evaluación de un nuevo análisis de riesgos ante los virus gusano (worms) y una mejora continua de las soluciones implementadas en su institución educativa?	NO	NO	NO

Tabla 5.6 Relación de comparación de la variable "mejoras de las acciones ante la problemática" en tres segmentos de estudio.

Capítulo 6

Conclusiones

En este capítulo se darán a conocer las conclusiones obtenidas en el estudio en general. Adicionalmente se pretende dar pauta a nuevas inquietudes y futuros estudios.

6.1 Conclusiones del estudio

Se realizó un estudio exploratorio acerca de la conciencia del problema que son los virus gusano (worms) en las universidades de México y cómo se atiende a estos problemas. Concluyendo la hipótesis número 1 "Los virus gusano (worms) al propagarse en la red de una universidad impactan económicamente a la institución educativa y reducen la productividad de las actividades en una computadora" se tiene:

a) Mientras más grande sea la población de computadoras en una institución más grande es el problema de los virus gusano (worms).
b) El impacto económico y productivo de los virus gusano (worms) es directo a las universidades que tienen un modelo educativo y sistemas administrativos con sustento en las tecnologías de información.

No se está evaluando el método; por lo tanto no podemos hacer afirmaciones acerca de su viabilidad. Sin embargo, se evalúo los elementos constitutivos que se proponen del método, que si bien son evaluaciones de seguridad informática usadas en las industrias; las universidades de México no realizan ningún análisis.

La hipótesis número 2 "Las universidades de México no cuentan con las medidas de seguridad y análisis que se sugieren en la consultoría a empresas sobre seguridad informática" se concluye es verdadera con el análisis del capítulo 5.

El método que se propuso se muestra en la figura 6.1 y al realizar la evaluación de sus componentes esenciales y de qué debería tener cada análisis propuesto, se concluye que el método puede ser adecuado para las expectativas de seguridad de las universidades de México.

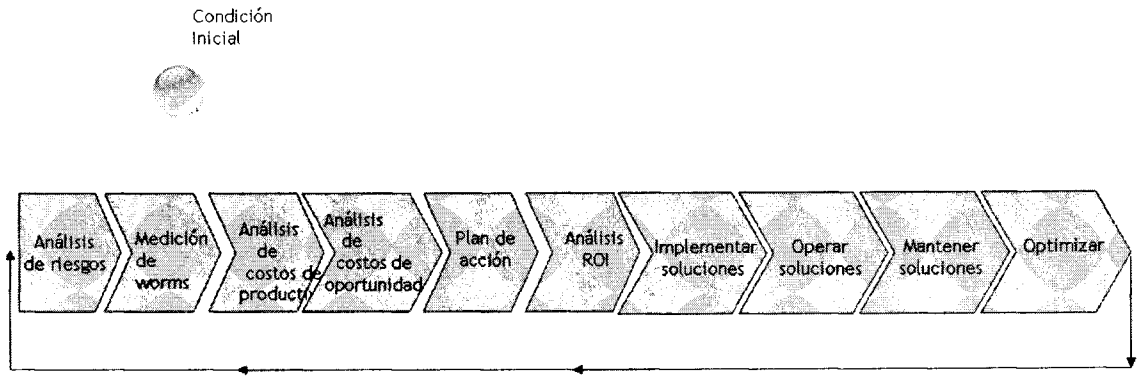


Figura 6.1 Método propuesto en el estudio de tesis.

El objetivo "Diseñar un método que permita prevenir y detectar la propagación de virus gusano (worms) para mitigar el impacto económico y mantener la productividad al ser implementado en las universidades de México" se cumple en este estudio de tesis teniendo como producto final dicho método, dirigido a las personas de tecnologías de información y al personal directivo de las universidades de México, campis del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) y miembros activos de la Corporación Universitaria para el desarrollo de Internet A. C. (CUDI), interesadas en ofrecer un ambiente mínimo de incidentes causados por los virus gusano (worms).

Se espera que lector pueda encontrar en este estudio, una forma diferente de tratar la seguridad informática, en general, de las universidades de México.

6.2 Futuros trabajos e investigaciones

El estudio de la seguridad informática es importante pero al igual delicado por la exposición de información que pudiera comprometer a la institución. La tesis no revela este tipo de información ni compromete a terceras personas.

La implementación del método para concluir su viabilidad es el trabajo futuro de esta investigación.

Anexo A

Encuesta

INTRODUCCION:

Hola que tal,
Soy Ramiro Alejandro Bermúdez Uribe estudio la maestría en Administración de Tecnologías de Información en el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) Campus Guadalajara y estoy realizando un estudio para la elaboración de mi tesis.

Dicho estudio no trata de evaluar a la persona que realiza este cuestionario; sino reunir información relevante sobre el conocimiento, la administración y el enfoque de seguridad específicamente en la amenaza de los virus gusanos (worms).

Se pretende realizar un análisis objetivo con un enfoque de negocio (oportunidades, pérdidas, productividad y administración de riesgo) y con su apoyo tecnológico (mediciones, tecnología y herramientas) para poder presentar después una metodología que conjunte los dos ámbitos y se pueda generar estrategias sustentables y paulatinas para minimizar el impacto económico que pueden generar los worms y mantener la productividad en una universidad.

La herramienta para este estudio es una sencilla encuesta que sólo le tomará 5 minutos en contestarla y la cual se encuentra en formato electrónico.

Agradezco el tiempo que dedica a este estudio.

DATOS GENERALES DEL ENCUESTADO:

Nombre (opcional):
Universidad (opcional):
Rol en la universidad:

a) Técnico
b) Gerencia media (dirección de informática)
c) Gerencia alta (director general)

INFORMACION GENERAL DE LA PROBLEMÁTICA

1. ¿En su institución educativa tiene problemas de virus gusano (worm)?
   - Demasiados.
   - . Muy importantes.
   - . Importantes.
   - . Poco importantes.
   - . Ninguno

2, ¿Dónde afectan principalmente los virus gusano (worms) a su institución educativa?
   - Comunicación con las plataformas tecnológicas.
   - . Impresión por red.
   - . Voz sobre Ip (VOIP), Telefonía IP y servicios sensibles al retraso.
   - . Denegación de servicio (DOS).
   - Saturación de enlaces.
   - Corrupción de datos en equipo de cómputo.
   - Baja productividad en el personal debido a remover los virus gusano (worms).
   - Todas las respuestas aplican.

3. ¿Cuáles son los mecanismos de adquisición de virus gusano (worms) que tiene identificados y que suceden en su institución educativa?
   - Adquisición en red por vulnerabilidades en el sistema operativo.
   - Ejecución de archivos contaminados.
   - Correo electrónico (mail) con archivos adjuntos.
   - Aceptación de archivos por mensajería instantánea.
   - Vulnerabilidades en la visualización de archivos gráficos con terminación .jpg
   - Uso de programas p2p (peer-to-peer) para compartir archivos.
   - Todas las anteriores respuestas suceden en mi institución educativa.
   - No conozco ninguna que suceda.

CUANTIFICACIÓN DE LA PROBLEMÁTICA

4. ¿Realiza alguna medición de máquinas vulnerables a un virus gusano (worm) en su institución educativa?

- NO.
- SI.

5. De ser afirmativa la pregunta anterior, ¿cuál es el porcentaje de máquinas vulnerables en su red?

- 0%
- 10%
- Entre 20% y 50%
- Entre 50% y 80%
- Todas las máquinas son vulnerables.

6. ¿Realiza alguna medición de máquinas con virus gusano (worm) que generen tráfico a sus enlaces?

- NO.
- SI.

7. De ser afirmativa la pregunta anterior, ¿cuál es la proporción de tráfico de paquetes de red que es generado por los virus gusano (worm)

- No hay tráfico de worms.
- 0-10%
- 11%-20%
- 21%-50%
- 51%-60%
- 61%-90%
- 98%

8. ¿Cuánto tiempo le toma, en promedio a sus técnicos, reparar una máquina que por alguna razón contrajo un virus gusano (worm)?.

- 1 hora.
- 2 horas.
- 3 horas.
- Más de 4 horas.

TRATAMIENTO AL PROBLEMA

9. En su institución educativa ¿Qué tan frecuente existen reuniones del personal de tecnologías de información (TI) cuyo objetivo es la seguridad informática?

- Nunca.
- De 1 a 5 veces al año.
- De 6 a 10 veces al año.
- Más de 10 veces al año.

10. ¿Realiza en su institución educativa un análisis de riesgos para contemplar la amenaza de los virus gusanos (worms)?

- NO.
- . SI.

11. Señale los factores que considera importantes en un análisis de riesgos para evaluar la amenaza de los virus gusano (worms).

- Contempla dispositivos vulnerables y fuentes de riesgos.
- Frecuencia y probabilidad de aparición de virus gusano (worms).
- Disponibilidad de equipos.
- Criticidad de activos.
- Impacto al negocio.
- Tiempos muertos en el trabajo de las personas.
- Todos los anteriores.
- Ninguno de los anteriores.

12. ¿Su institución educativa cuenta con una política de seguridad informática que ampare estrategias de seguridad en contra de los virus gusano (worms)?

- NO.
- . SI.

13. De ser afirmativa la pregunta anterior, ¿cuál es el alcance que tiene las reglas o estatutos de la política de seguridad de su institución educativa?

- Es un documento que es conocido sólo por el área de tecnologías de información TI.
- Se aplican las reglas con excepciones.
- No tiene carácter obligatorio.
- Es aplicable para los alumnos y personal administrativo pero no así con los directivos.
- Las sanciones no tienen importancia o se condonan fácilmente.
- No existe compromiso de la alta y media gerencia,
- Todas las anteriores,
- Ninguna de las anteriores.

14. ¿Realiza en su institución educativa un análisis de costos en la productividad para contemplar la amenaza de los virus gusanos (worms)?

- NO.
- SI.

15. Señale los factores que considera importantes en un análisis de costos en la productividad para evaluar la amenaza de los virus gusano (worms).

- Relación tiempo/costo de técnicos en reparar equipo.
- Pérdida de información.
- Relación tiempo/productividad por no realizar actividades.
- Disponibilidad de recursos críticos.
- Imagen de la institución educativa.
- Todos los anteriores.
- Ninguno de los anteriores.

16. ¿Realiza un estudio de los costos de oportunidad para contemplar la amenaza de los virus gusanos (worms)?

- NO.
- SI.

17. Señale los factores que considera importantes en un análisis de costos de oportunidad para evaluar la amenaza de los virus gusano (worms).

- Disponibilidad de recursos que pudiera impedir una entrada económica a la institución educativa. Por ejemplo, si se ofrece un diplomado y el sistema de tesorería no se encuentra disponible, ocasiona que se pierda un ingreso de colegiatura de un aspirante a este diplomado.
- Imagen que presenta la institución educativa.
- Costo perdido por reparar fallas.
- Costo por improductividad en el personal.
- Costo de ancho de banda (enlaces) mal usado.
- Otros_____
- Todos los anteriores.
- Ninguno de los anteriores.

ACCIONES ANTE LA PROBLEMÁTICA

18. Ante una amenaza de virus gusano (worms) ¿cuál es su comportamiento para minimizar o quitar dicha amenaza en su institución educativa?

- Se realizan actividades reactivas para erradicar a los worms.
- Se realizan actividades proactivas para erradicar a los worms.

- Se realiza una combinación de actividades reactivas y proactivas para erradicar a los worms.
- No realizo ninguna actividad.

19. Señale algunas actividades que realiza para minimizar la amenaza de los virus gusano (worms).

- Instalación de un firewall.
- Bloqueo de máquinas generadoras de tráfico dañino.
- Instalación de un antivirus en máquinas.
- Actualización del sistema operativo.
- Actualización de paquetería Office de Microsoft.
- Configuraciones en clientes de correo para combatir worms.
- Instalación de software antispyware.
- Campañas de educación.
- Sigo la recomendación del 1,2,3 de Microsoft.
- Sigo la recomendación del 1-12 de Trend (compañía de antivirus)
- Integración de máquinas a un dominio de Microsoft y aplicación de actualización por Microsoft Software Update Services (SUS).
- Integración de herramientas como NAC (Cisco Network Admission Control) y CSA (Cisco Security Agent).
- Segmentación lógica de la red (vlans).
- Uso de tecnología 802.1x
- Uso de herramientas open source (código abierto) para detectar máquinas vulnerables.
- Uso de tecnología IDS (Sistema de Detección de Intrusiones).
- Uso de tecnología IPS (Sistema de Prevención de intrusiones).
- Correlación de alarmas entre herramientas de monitoreo, IDS e IPS.
- Uso de tecnología de vlans dinámicas.
- Uso de tecnología Private VLANs.
- Acceso controlado de máquinas a la red (registro de red).
- Monitoreo de peticiones de nombre por máquina al DNS (Servidor de solución de nombres).

20. ¿Realiza un estudio de viabilidad económica cuando contempla soluciones ante los virus gusano (worms)?

- NO.
- SI.

21. De ser afirmativa la pregunta anterior, mencione los elementos de su análisis de viabilidad económica.

- Estudio del retorno de la inversión (ROI).
- Estudio del valor presente neto (NPV).
- Otro_____

22. Al implementar, operar y mantener sus actividades para minimizar los virus gusano (worms) ¿contempla personas, procedimientos y tecnología?

- NO.
- . SI.

MEJORA DE LAS ACCIONES ANTE LA PROBLEMÁTICA

23. Al implementar, operar y mantener las soluciones para minimizar virus gusano (worms) se realiza un esfuerzo importante económico, tecnológico y educativo. ¿Realiza un estudio de costo-beneficio de las soluciones y actividades para evaluar objetivamente si el esfuerzo vale la pena?

- NO.
- . SI.

24. ¿Existe un ciclo de retroalimentación, evaluación de un nuevo análisis de riesgos ante los virus gusano (worms) y una mejora continua de las soluciones implementadas en su institución educativa?

- NO.
- . SI.

GRACIAS POR SU TIEMPO EN LLENAR ESTA ENCUESTA.

Si desea saber el resultado final del análisis de esta recolección de información, favor de consultar la página http:// que mantendrá un reporte de este análisis hasta el día x de septiembre de 2005.

GLOSARIO DE TÉRMINOS DE LA ENCUESTA:

Virus Gusano (worm): es un virus o programa que no altera los archivos sino que reside en la memoria y se duplica a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Análisis costo-beneficio: evaluación objetiva de las ganancias y beneficios involucrados en el proyecto.

Análisis de costos en la productividad: relación económica en los logros de la fuerza de trabajo.

Análisis de costos de oportunidad: el costo de oportunidad de producir algo es igual al valor de las producciones alternativas a las que se renuncia para obtenerlo.

Análisis de riesgos: lidentificar, analizar y administrar las fuentes de riesgos antes de que empiecen ha amenazar el funcionamiento continuo y confiable de los sistemas de información.

Análisis de viabilidad económica: factibilidad de realizar un proyecto económicamente.

Política de seguridad: es un código de conducta para la utilización de un sistema de información que trata de evitar accidentes.

802.1x: IEEE 802.1X es un estándar basado en el control y acceso de puertos en la red. Provee autenticación a los dispositivos conectados en la red para establecer una conexión punto a punto o negar la conexión si la autenticación es errónea.

Activos: es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios.

Algoritmo: es un conjunto finito de instrucciones o pasos que sirven para ejecutar una tarea o resolver un problema. La palabra algoritmo deriva del nombre del matemático árabe Al Juarismí, que vivió entre los siglos VIII y IX.

Antispyware: Estos programas son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. Una forma común de instalación es por virus o mediente la ejecución de programas que contienen este spyware. Un Antispyware es un programa que elimina este tipo de espía.

Bit: Binary Digit (dígito binario). Un bit es la unidad mínima de información empleada en informática. Cuatro bits forman un nibble, y ocho bits forman un byte u octeto.

Cliente: programa u ordenador que accede a recursos y servicios brindados por otro llamado Servidor, generalmente en forma remota.

CSA: Cisco Security Agent es un programa cuya función es suministrar protección contra amenazas a los servidores y estaciones de trabajo. El agente identifica y evita todo comportamiento maligno, eliminando de esta manera los peligros a la seguridad.

Denegación de servicio (DOS): apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

DNS: el servidor de nombres (*Domain Name System*) es un conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

Firewall: Un cortafuegos o firewall en inglés, es un equipo de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario.

Hardware: se refiere a todos los componentes físicos (que se pueden tocar) de la computadora: discos, unidades de disco, monitor, teclado, mouse, impresora, placas, chips y demás periféricos.

IDS: son las siglas de Intrusion Detection System, en inglés Sistema de Detección de Intrusiones. Estos son programas que revisan el estado del sistema y que reportan cuando existe peligro en él.

Intangibles: activos que no se pueden identificar físicamente pero que tienen la capacidad de generar ventajas competitivas sostenibles en el tiempo. Ejemplos de éstos son: el dominio de un tema o la experiencia de una persona.

Internet: es una red de redes a escala mundial de millones de computadoras interconectadas.

IP (Protocolo Internet): es un protocolo orientado a datos usado tanto por la fuente como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

IPS: son las siglas de intrusion prevention system, en inglés. Sistema de prevención de intrusiones. Estos son programas que revisan las conexiones antes de que lleguen a un sistema y reportan cuando existe peligro para él.

JPEG (Joint Photographic Experts Group): es un algoritmo diseñado para comprimir imágenes con 24 bits de profundidad o en escala de grises. JPEG es también el formato de archivo que utiliza este algoritmo para comprimir imágenes. El formato de archivos JPEG se abrevia frecuentemente **JPG** debido a que algunos sistemas operativos sólo aceptan tres letras de extensión.

LAN: local area network, red de área local.

Mensajería instantánea: son un conjunto de programas que sirven para enviar y recibir mensajes instantáneos con otros usuarios conectados a Internet, además saber cuando están disponibles para hablar. Algunos ejemplos son: Los ICQ, Yahoo! Messenger, MSN Messenger y AIM (Aol Instant Messenger).

NAC: Cisco Network Admission Control (NAC) es un programa de múltiples proveedores enfocado en limitar el daño ocasionado por las amenazas emergentes de seguridad tales como virus y gusanos. Con NAC, los clientes pueden restringir los accesos de red para los dispositivos de punto final confiables y que cumplan con ciertas políticas y pueden prohibir el acceso de los dispositivos que no cumplan con las políticas.

NPV: Es una herramienta para calcular el descuento del flujo de efectivo.

Open Source: Código abierto (*open source* en inglés) es el término por el que se conoce al software distribuido y desarrollado en una determinada forma. Este término empezó a utilizarse en 1998 por algunos usuarios de la comunidad del software libre, tratando de usarlo como reemplazo al ambiguo nombre original, en inglés, del software libre (free software) terminología introducida por Richard Stallman

Private VLANs: concepto de aislar máquinas de un segmento; es decir, no existe comunicación entre una máquina a otra aunque se encuentren en el mismo segmento de red (VLAN).

p2p (peer-to-peer): se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red. Ejemplos de estos programas son: Kazza, Gnutella o Napster.

ROI: (Return of Investment) Retorno de la inversión. Es una herramienta de toma de decisiones de inversión utilizada para comparar la factibilidad económica de diferentes opciones.

Servidor: una computadora que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes.

Software: es la parte lógica de la computadora. Conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina.

SUS: Microsoft Software Update Services (SUS) es un programa diseñado para simplificar el proceso de mantener sistemas basados en Windows con la última actualización crítica de seguridad. SUS habilita a los administradores para desplegar rápidamente y de forma segura las actualizaciones de seguridad en sus plataformas de servidor Windows 2000 Server así como en las plataformas de escritorio Windows 2000 Professional y Windows XP Professional.

Tangible: Activos que se pueden identificar y valorar debido a que tienen un soporte físico y se concretan en algo material.

Tecnologías de información: son la serie de metodologías, herramientas, técnicas y dispositivos utilizados en el manejo y proceso de la información, dentro del ámbito de la informática y la computación.

Telefonía IP: sistema avanzado de comunicaciones empresariales, que utilizando IP como medio de transporte, permite crear un sistema telefónico con todas las funciones de un PBX (conmutador) tradicional, y agrega nuevas funcionalidades como integración de aplicaciones vía XML, distribución inteligente de la fuerza de trabajo, automatización de la administración, movilidad, etc.

VLAN: concepto de segmentación lógica en una red. Virtual LAN. Dominio de broadcast.

Virtual: coloquialmente virtual tiene un significado similar a cuasi o seudo particularmente cuando se usa en forma adverbial.

VOIP: transporte de voz encapsulada dentro de paquetes de datos utilizando el protocolo de internet (IP) sobre redes públicas o privadas.

Web: La World Wide Web (del inglés, Telaraña Mundial), la Web o WWW, es un sistema de hipertexto que funciona sobre Internet.
XML: es el acrónimo del inglés eXtensible Markup Language (lenguaje de marcado ampliable o extensible). Su objetivo principal es conseguir una página web más semántica.

Anexo B

Como realizar mediciones de virus gusano (worms). Investigación realizada para el estudio de tesis y asesorada por el departamento de servicios de redes y telecomunicaciones de la Vicerrectoría de Tecnologías de infomación del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM)

A) Listas de acceso: genera una simple lista de acceso en tu router.

Sintaxis Cisco en un router

```
no access-list 126
access-list 126 remark trafico al corporativo
access-list 126 permit   tcp any any range 135 139
access-list 126 permit  udp any any range 135 139
access-list 126 permit   tcp any any range 1433 1434
access-list 126 permit   udp any any range 1433 1434
access-list 126 permit   tcp any any eq 445
access-list 126 permit   udp any any eq 445
access-list 126 permit ip any any


interface FastEthernet1/1
ip access-group 126 in
```

Sintaxis Cisco en un pix

```
object-group network Universidad
  description Bloque de Ip's de Universidad
  network-object 10.49.128.0 255.255.224.0

object-group service worm_udp udp
  port-object range 135 139
  port-object eq 445
  port-object range 1433 1434

object-group service worm_tcp tcp
  port-object range 135 netbios-ssn
  port-object eq 445
  port-object range 1433 1434

access-list vpn_in remark Negado de puertos TCP
access-list vpn_in permit tcp any any object-group worm_tcp
```

```
access-list vpn_in remark Negado de puertos UDP
access-list vpn_in permit udp any any object-group worm_udp
access-list vpn_in remark Permitir bloque de la universidad
access-list vpn_in permit ip object-group Universidad any
access-list vpn_in deny ip 10.0.0.0 255.0.0.0 any

access-group vpn_in in interface inside
```

Consideraciones:

- Estas listas son únicamente para ver que cantidad de tráfico para por una interfase y es catalogado como trafico de virus gusano (worms).

- Si se tuviera un servidor de correo Exchange se debe de permitir antes la dirección ip de éste. El mismo caso será para accesos a una base de datos con msql a la universidad.

- Se contabiliza tres virus gusano (worms) muy conocidos, fácil de detectar y además que originan mucho tráfico. Estos son el blaster, sasser y slammer.

- Los protocolos usados son el UDP (*User Datagram Protocol*) y el TCP (Transmission Control Protocol)

Definiciones:

UDP Siglas de *User Datagram Protocol.*

Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Se utiliza cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

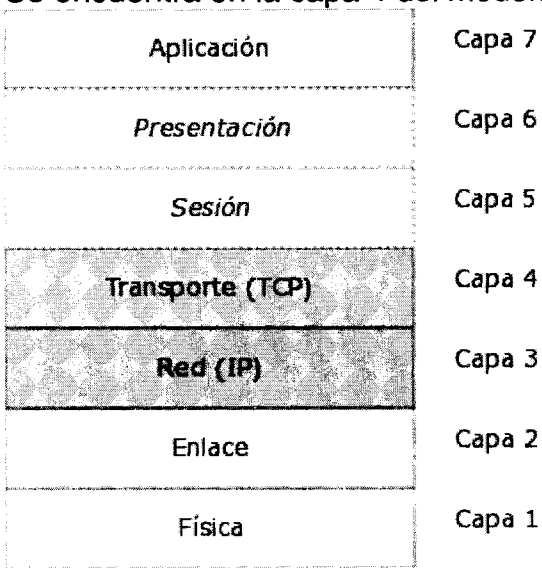
No usa acuse de recibo en las transacciones entre computadoras.

Comentado en RFC 768 (*http://www.ietf.org/rfc/rfc0768.txt*)

TCP. Protocolo de control de transmisión (Transfer Control Protocol). Es el protocolo que se encarga de la transferencia de los paquetes a través de Internet. Se encarga de que los paquetes lleguen al destino sin ningún error o pide su reenvío. Se encarga de la capa de transporte del modelo.

Comentado en RFC 793 (*http://www.ietf.org/rfc/rfc0793.txt*)

Se encuentra en la capa 4 del modelo OSI



Tomado de http://es.wikipedia.org/wiki/UDP

Las referencias de los puertos que usan los virus gusano (worms) son:
Puerto 455 Sasser
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.A
Puerto 1433 y 1434 Slammer
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FSQLP1434%2EA&VSect=T
Puerto 135 al 139 Blaster
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

B) NBAR Network-Based Application Recognition

http://www.cisco.com/warp/public/cc/so/neso/ienesv/cxne/nbar_ov.htm

Realizar el mismo ejercicio de las listas del punto A.

Voice1#show ip nbar proto top-n 5

Ethernet0/0

Protocol	Input Packet Count Byte Count 5 minute bit rate (bps)	Output Packet Count Byte Count 5 minute bit rate (bps)
telnet	1531	0
	91860	0
	0	0
netbios	78	0
	9783	0
	0	0
custom-01	8	0
	486	0
	0	0
napster	4	0
	240	0
	0	0
bgp	0	0
	0	0
	0	0
unknown	6	0
	360	0
	0	0
Total	1627	0
	102729	0
	0	0

C) Netflow Capacidad de los routers cisco para mandar información de tráfico.

http://www.cisco.com/warp/public/732/Tech/nmp/netflow/index.shtml

Netflow es una tecnología eficiente que provee una contabilidad de nuestra red.

- Estadísticas de tráfico de red.
- Facturación del uso de la red.
- Planeación de la red.
- Monitoreo de red.
- Sentido de las conexiones.
- Iniciativas para el Enterprise QoS y records de Type of Service (ToS)

Existen dos herramientas en Cisco para el análisis de flujo.

- Neflow Collector.

- Netflow Analyzer.

Para mayor detalle de Netflow consultar la liga
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm

En el router:
conf ter
interfase fast0/0
ip route-cache flow
end
!blaster
show ip cache flow | include 0087
!sasser
show ip cache flow | include 01BD
!slammer
show ip cache flow | include 059A

Utilizar el comando *show ip cache flow* en los routers de core para identificar algunas PC con demasiadas conexiones o ataques a ciertos puertos. Nota: Para hacer uso de este comando se requiere habilitar dentro las interfases Vlan (o en alguna otra interfase) el comando *ip route-cache flow*.

MSFC-C1#sh ip cache flow

Vl24	*10.25.162.53*	*Vl37*	*200.66.249.212*	*06 0050 0BDA*	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.145*	*06 0CC6* ***0087***	*1*
Vl23	*10.25.161.184*	*Null*	*10.25.47.233*	*06 0870 0087*	*3*
Vl20	*10.25.158.150*	*Vl37*	*203.70.46.70*	*11 2AA5 29D5*	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.144*	*06 0CC4* ***0087***	*1*
Vl23	*10.25.161.184*	*Vl36*	*10.25.59.235*	*06 08FD 0401*	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.147*	*06 0CCD* ***0087***	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.148*	*06 0CCF* ***0087***	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.146*	*06 0CC8* ***0087***	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.150*	*06 0CD3* ***0087***	*1*
Vl10	***10.25.129.160***	*Vl37*	*10.25.76.149*	*06 0CD1* ***0087***	*1*
Vl10	***10.25.129.60***	*Null*	*10.25.224.213*	*06 0D57 01BD*	*2*
Vl10	*10.25.129.60*	*Null*	*10.25.161.81*	*06 0CF7 01BD*	*2*
Vl10	***10.25.129.60***	*Null*	*10.25.192.11*	*06 0DB2* ***01BD***	*1*
Vl10	***10.25.129.60***	*Null*	*10.25.112.130*	*06 0DBE* ***01BD***	*1*
Vl10	***10.25.129.60***	*Null*	*10.25.176.106*	*06 0DB5* ***01BD***	*1*
Vl10	***10.25.129.60***	*Null*	*10.25.16.47*	*06 0DC6* ***01BD***	*1*
Vl10	***10.25.129.60***	*Null*	*10.25.193.50*	*06 0CDD* ***01BD***	*2*

En el ejemplo anterior se observan varias conexiones desde una IP hacia varias IP atacando los puertos 0087 y 01BD, se recomienda revisar ese par de PC's

Nota: En algunas plataformas como el Catalyst 4006 o 4500 con supervisora III no existe información de netflow. Esta es necesaria obtenerla del router de Internet.

El comando ip route-cache flow muestra la información de los flujos de entrada a la interfaz (no de salida de esta)

Se puede poner Alias para ahorrarse líneas de comandos.

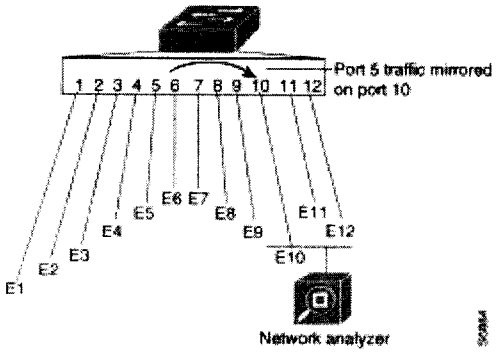
Conf ter
alias exec blaster show ip cache flow | include 0087
alias exec slammer show ip cache flow | include 059A
alias exec welchia show ip cache flow | include 0000
alias exec sasser show ip cache flow | include 1BD0

para visualizar
router#blaster
router#sasser

Herramienta de código abierto (open source)
http://www.ntop.org/

¿Qué es ntop?
Ntop es una herramienta que muestra el uso de la red muy similar al popular comando top de Linux. Trabaja en varias plataformas y provee información valiosa de troubleshooting a los administradores de red en un servidor de web.
Configuraciones en los dispositivos cisco para mandar datos:

1. Si es un tipo recortado de analizador de protocolos sería necesario poder tener información de varias vlans o host de la red. Para ello necesitamos poner un puerto de Switched Port Analyzer (**SPAN**) para alimentar a NTOP de información de varios host.



- 6509 -> set span 2-3,6,8 4/43 rx inpkts disable learning enable multicast enable create

OJO: 2-3,6,8 son las vlans 4/43 es el puerto que alimenta al 6509. El 6509 tiene en este caso conocimiento de todo el tráfico.

- 3550, 3500, 2950, 2900 -> Switch(config)# **monitor session 1 source interface fastethernet 5/1**

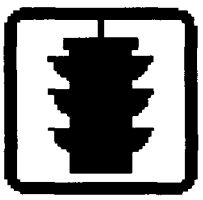
y

Switch(config)# **monitor session 1 destination interface fastethernet 5/48**

OJO: source es la interface que nos pueda ofrecer varios datos; por ejemplo la que alimenta al router de lan. Destination es el puerto que alimenta al stop.

- 4006-> set span 2-3,6,8 4/43 rx inpkts disable learning enable multicast enable create

OJO: El mismo caso que para el 6509.



Si se pone esta opción hay que recordar que es demandante para la red. ESTO ES SÓLO PARA DIAGNÓSTICO EN UNA CONTIGENCIA no para tener permanentemente un monitoreo que puede causar inestabilidad en el switch fuente tanto en arp, incrementos de cpu y problemas en capa 2 (enlace).

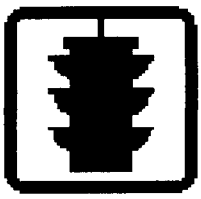
2. Por netflow mandado desde el router que posee información.

Router(config)#ip flow-export destination 10.40.a.b 2055
Router(config)#ip flow-export version 5

Y poner el comando "ip route-cache flow" en el la vlan de diagnostico.

interface Vlan2
description VLAN INTERNET
ip route-cache flow

* En lo encontrado en la documentación de internet se menciona que ntop trabaja con la versión 5 del netflow.


El "ip flow-export destination 10.40.a.b 2055" en el router es bueno dejarlo mientras se hace el análisis y se saca conclusiones. Dependiendo de la memoria y de la capacidad de la máquina del Ntop podrá abortar el proceso si se exceden sus capacidades.

Herramienta comercial
http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/index.html

D) Estadísticas con el Switch

Usando el comando *show interface | include packets input.* Podemos ver el histórico de los paquetes recibidos de cada una de las interfases que tiene el sw o router. Se recomienda limpiar los contadores antes de usar este comando *clear counters.* Este comando es útil usarlo en cualquier switch y no hay que activar nada en las interfaces.

```
C3550-24-TRAILER#sh int | inc packets input
    0 packets input, 0 bytes, 0 no buffer
    9 packets input, 862 bytes, 0 no buffer
    0 packets input, 0 bytes, 0 no buffer
    0 packets input, 0 bytes, 0 no buffer
    0 packets input, 0 bytes, 0 no buffer
    555 packets input, 100720 bytes, 0 no buffer
    0 packets input, 0 bytes, 0 no buffer
    0 packets input, 0 bytes, 0 no buffer
    0 packets input, 0 bytes, 0 no buffer
    16 packets input, 1194 bytes, 0 no buffer
    26 packets input, 1694 bytes, 0 no buffer
    26 packets input, 1688 bytes, 0 no buffer
```

En el ejemplo anterior se limpio los contadores y después de 3 segundos, vemos que la interfase número 5 contiene demasiado tráfico. Se recomienda buscar que switch o que equipo está conectado ahí.

E) Contabilización de paquetes en la interface del router

Conf ter
Interfase fa0/0
ip accounting

Utilizar el comando *show ip accounting*, con esto despliega históricamente el número de paquetes que ha transmitido cada una de las conversaciones actuales, se recomienda limpiar el accounting antes de consultar este comando *clear ip accounting.* Para utilizar este comando se debe activar el accounting en cada una de las interfases que se requiere con: *ip accounting output-packets.* Se recomienda filtrar el resultado con | *include* o | *exclude*

gwtolwan_#sh ip accounting

Source	*Destination*	*Packets*	*Bytes*
132.254.96.2	*137.132.231.242*	*12*	*582*
132.254.96.2	*68.52.113.25*	*72*	*3456*
132.254.96.2	*219.95.98.250*	*23*	*1104*
132.254.96.2	*216.155.193.159*	*295*	*21540*
132.254.96.2	*24.101.44.76*	*245*	*11760*
132.254.101.65	*64.12.174.185*	*3*	***80***
132.254.96.2	*129.59.56.159*	*21*	*1032*
132.254.96.2	*24.174.217.114*	*15*	*720*
132.254.96.2	*148.233.203.171*	*51*	*2447*

En el ejemplo anterior se limpio contadores y después de 5 segundos se ejecutó el comando, vemos que la IP *132.254.96.2* tiene demasiadas conversaciones hacia Internet y la cantidad de paquetes es muy alta para 5 segundos.

F) Analizadores de protocolos

De forma similar a NTOP con el uso del Switched Port Analyzer (**SPAN**) trabajar con soluciones comerciales y código abierto (open source).

Comerciales:
1) NAM hardware CISCO
2) Etherpeek http://www.wildpackets.com/
3) Sniffer http://www.networkgeneral.com/

Código abierto (Open Source)
http://www.ethereal.com/

G) Monitoreo de tráfico por puertos de worms usando herramientas
SolarWinds Orion, NetScout Performance Reporting, Concord, MRTG o Cricke.t
Estas dos últimas código abierto (open source).

H) Análisis wireless

Comerciales:

Airopeek

http://www.wildpackets.com/solutions/wireless

Código abierto (open source)

http://www.linuxlinks.com/Software/Networking/Tools/Wireless/

Bibliografía

Anónimo (agosto 24, 2004) Virus is no.1 source of financial loss. *Information System Security Society of the Philippines* Consultado el 30 de octubre del 2004 de: http://www.isssp.org.ph/articles-virus1.htm

Anónimo (n. d.) Virus Informáticos. *Instituto Tecnológico de Querétaro* consultado el 4 de noviembre del 2004 de: http://www.itq.edu.mx/vidatec/espacio/aisc/ARTICULOS/virus/VIRUS.htm

Anónimo (2003) Portafolio de consultoría y soporte de técnico *Internet Solutions* consultado el 5 de noviembre del 2004 de: http://www.internet-solutions.com.co/Servicios%20Consultoria%20y%20Soporte.pdf

Anónimo (2004, mayo 3) Worms to cost service providers $245 million in 2004; Study shows attacks on ISPs now a daily occurrence. *M2 Communications Ltd, Sandvine Inc* consultado el 30 de enero del 2005 de: http://0-proquest.umi.com.millenium.itesm.mx/pqdlink?index=2&did=569126051&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1107118878&clientId=23693

Arámbulo, A. (2005) Consultora Dicta. Consultado el 5 de marzo del 2005 de: http://www.dicta.com.mx

Acohido B. y Swartz J. (2004, sep 09) Microsoft's SP2 won't cure all security ills. *USA Today (n.d)* consultado el 10 de octubre del 2004 de: http://www.crmassist.com/news/dispnews.asp?i=120853&t=99

Ballem, J. (2004, enero 09) Reggie, *Universidad de Brown.* consultado el día 30 de junio de: http://www.brown.edu/Facilities/CIS/Projects/netreg/reggie/

Bradner S.(Jun 21, 2004) Estimating the cost of a Windows Armageddon *Network World.* Framingham (Jun 21, 2004) Vol.21, Iss. 25; pag. 34 consultado el 5 de noviembre del 2004 de: http://0-gateway.proquest.com.millenium.itesm.mx:80/openurl?url_ver=Z39.88-2004&res_dat=xri:pqd&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&rft_dat=xri:pqd:did=000000655019301&svc_dat=xri:pqil:fmt=html&req_dat=xri:pqil:pq_clntid=23693

Briesemeister L., Lincoln P. y Porras P (2003) Epidemic profiles and defense of scale-free networks *ACM Press New York, NY, USA (2003)* SESSION: Defensive technology, Pag: 67 - 75 consultado el 28 de septiembre del 2004 de:
http://0-delivery.acm.org.millenium.itesm.mx/10.1145/950000/948200/p67-briesemeister.pdf?key1=948200&key2=9346207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Carrillo J. (2002) Sistemas de desarrollo de prácticas de valor. Centro de sistemas de conocimiento. Tecnológico de Monterrey. Consultado el 30 de octubre del 2004 de
http://www-csc.mty.itesm.mx/Materiales_de_Difusion/archivos_pdf/notas_tecnicas/2000_PDF/csc2000_01.pdf

Castañeda F., Can Emre. y Xu Jun. (2004) WORM vs. WORM: Preliminary Study of an Active Counter-Attack Mechanism, *ACM Press, New York, NY, USA (2004)* Session 4, Pag. 83-93 consultado el 7 de noviembre del 2004 de:
http://0-delivery.acm.org.millenium.itesm.mx/10.1145/1030000/1029631/p83-castaneda.pdf?key1=1029631&key2=8231489901&coll=portal&dl=ACM&CFID=30948046&CFTOKEN=68468823

Chen T. y Robert, J. (junio, 2004) Worm epidemics in high-speed networks *Computer and Communications Societies. IEEE (junio, 2004),* Volume: 37, Issue: 6 Pag. 48 – 53 consultado el 29 de octubre del 2004 de:
http://0-ieeexplore.ieee.org.millenium.itesm.mx/iel5/2/28995/01306386.pdf?tp=&arnumber=1306386&isnumber=28995&arSt=48&ared=53&arAuthor=Chen%2C+T.M.%3B+Robert%2C+J.-M.%3B

Christodorescu M. y Jha S. (2004) Testing malware detectors *ACM Press New York, NY, USA (2003).* SESSION: Testing, Pag: 34 - 44 consultado el 30 de septiembre del 2004 de:
http://0-delivery.acm.org.millenium.itesm.mx/10.1145/1010000/1007518/p34-christodorescu.pdf?key1=1007518&key2=4593207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Christopher M., King, Curtis E. Dalton, T. Ertem Osmanoglu (2001). Security architecture : design, deployment and operations. Berkeley, CA: Osborne/McGraw-Hill, c2001.

Davis K. (2001).Saving users from themselves: creating an effective student-oriented anti-virus intervention *ACM Press New York, NY, USA (2001).* Session: Technical Sess, Pag: 27-32 consultado el 28 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/510000/500965/p27-davis.pdf?key1=500965&key2=7491207901&coll=portal&dl=ACM&CFID=28897295&CFTOKEN=55602418

Egan, M. (enero 17, 2004). ¿Ha revisado recientemente su programa de seguridad?. Symantec. Consultado el 15 de abril del 2005 de: http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_3133.html

Fomenkov M., Keys K., Moore D. y Claffy K. (2003) Longitudinal study of Internet traffic in 1998-2003 *Caida* consultado el 7 de octubre del 2004 de: http://www.caida.org/outreach/papers/2003/nlanr/nlanr_overview.pdf

Gallivan, M. (2000). Examining workgroup influence on technology usage: a community of practice perspective. *ACM Press New York, NY, USA (2000).* SESSION: Special Interest Group on Computer Personnel Research Annual Conference. Pag: 54-66 consultado el 6 de mayo del 2005 de: http://0-portal.acm.org.millenium.itesm.mx/ft_gateway.cfm?id=333356&type=pdf&coll=portal&dl=ACM&CFID=54720557&CFTOKEN=30049704

Gordon, L. y Smith, R. (marzo 6, 2003) Econmic Aspects of Information Security. University of Maryland, College Park. Consultado el 3 de marzo del 2005 de: http://www.umiacs.umd.edu/docs/umiacspresentation.pdf

Gunasekaran, A,, Khalil, O. y Mahbubur R. (2003) "Knowledge and Information Technology Management, Human and Social perspectives", editado por Idea Group Publishing, 2003.

Henning R. (1999) Security service level agreements: quantifiable security for the enterprise?
ACM Press New York, NY, USA (1999). Pag: 54-60 consultado el 29 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/340000/335194/p54-henning.pdf?key1=335194&key2=8902207901&coll=portal&dl=ACM&CFID=28897295&CFTOKEN=55602418

Hery, W. (2005). SecurityMetrics. ISIS. Consultado el 4 de marzo de 2005 en: http://isis.poly.edu/courses/cs996-managements2005/Lectures/SecurityMetrics.ppt

Hopkins D (2000) Web Documentation Project at the University of Delaware *ACM Press New York, NY, USA (2000).* ACM Special Interest Group on University and College Computing Services, Pag: 102-105 consultado el 30 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/360000/354932/p102-hopkins.pdf?key1=354932&key2=5338737901&coll=portal&dl=ACM&CFID=28879398&CFTOKEN=7495717

King, C.,Dalton. C, y Osmanoglu T. (2001) Security Architecture. Design, Deployment & Operations. Mc Graw Hill

Krane, J. (2003, Sep 11). Computer-heavy electrical grid vulnerable to hackers, virases. The *Associated Press.* consultado el 20 de septiembre del 2004 de: http://www.securityfocus.com/news/6940

Labbé J. (2004). Servicio Impuestos Internos. Consultado el 14 de junio del 2005 de: http://www.netmedia.info/bsecure/articulos.php?id_sec=48&id_art=4915&num_page=21940

Lai Shou-Chuan, Kuo Wen-Chu y Hsieh Mu-Cheng (2004) Defending against Internet Worm-like Infestations. *Computer.org IEEE 18th International Conference on Advanced Information Networking and Applications (AINA'04) Volume 1* Consultado el 10 de noviembre del 2004 de: http://csdl.computer.org/comp/proceedings/aina/2004/2051/01/205110152abs.htm

Lei K y Rawles P. (2003) Strategic decisions on technology selections for facilitating a network/systems laboratory using real options & total cost of ownership theories *ACM Press New York, NY, USA (2003).* consultado el 10 de octubre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/950000/947139/p76-lei.pdf?key1=947139&key2=7463447901&coll=portal&dl=ACM&CFID=29161257&CFTOKEN=19544544

Liljenstam M., Nicol M., Berk V. y Gray R. (2003) Simulating realistic network worm traffic for worm warning system design and testing *ACM Press, New York, NY, USA (2003)* SESSION: Network interactions, Pag 24-33 consultado el 2 de noviembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/950000/948193/p24-liljenstam.pdf?key1=948193&key2=2510640011&coll=portal&dl=ACM&CFID=31150506&CFTOKEN=33895484

Mercuri R. (junio, 2003) Analyzing security costs *ACM Press, New York, NY, USA (junio, 2003)* COLUMN: Security watch Volume 46 , Issue 6 Pag. 15-18 encontrado el 2 de noviembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/780000/777327/p15-mercuri.pdf?key1=777327&key2=6742640011&coll=portal&dl=ACM&CFID=31150506&CFTOKEN=33895484

McCarthy, L. (diciembre 8, 2004) La importancia de las métricas de seguridad Symantec Corporation Consultado el 1 de marzo de 2005 en: http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_4619.html

McClure S., Scambray J. y Kurtz G. (2003) Hacking Exposed. (Tercera edición). Berkeley California: McGraw-Hill

McNamee, D. (n.d.) Glosario de Evaluación de Riesgo. Mc^2 Management Consulting. Consultado el 14 de junio del 2005 http://www.mc2consulting.com/riesgo.htm

Moore D., Paxson V., Savage S., Shannon C., Staniford S. y Weaver N. (2003) The Spread of the Sapphire/Slammer Worm. *Caida* consultado el 1 de octubre del 2004 de: http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

Moore D., Shannon C., Voelker G. y Savage S. (2003) Internet quarantine: requirements for containing self-propagating code INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE , Volume: 3 , 30 marzo-3 abril 2003 Pag:1901 - 1910 consultado el 30 de octubre del 2004 de: http://0-ieeexplore.ieee.org.millenium.itesm.mx/iel4/71/13289/00605765.pdf?tp=&arnumber=605765&isnumber=13289&arSt=781&ared=789&arAuthor=Roberts%2C+A.%3B+Symvonis%2C+A.%3B

Moore D., Paxson V., Savage S., Shannon C., Staniford S y Weaver N. (2003) Inside the Slammer worm Security & Privacy Magazine, IEEE (julio-agosto, 2003) Volume 1, Issue:4 Pag:33 – 39 consultado el 29 de octubre del 2004 de: http://0-ieeexplore.ieee.org.millenium.itesm.mx/iel5/8013/27399/01219056.pdf?tp=&arnumber=1219056&isnumber=27399&arSt=33&ared=39&arAuthor=Moore%2C+D.%3B+Paxson%2C+V.%3B+Savage%2C+S.%3B+Shannon%2C+C.%3B+Staniford%2C+S.%3B+Weaver%2C+N.%3B

Moulton B. (2004) Análisis de Riesgos. Symantec. Consultado el 12 de marzo de 2005 en: http://www.symantec.com/region/mx/enterprisesecurity/content/risks/LAM_3522.html

Neubauer B. y Harris J. (2002) Protection of computer systems from computer viruses: ethical and practical issues. *Journal of Computing Sciences in Colleges (October 2002)* Volume 18 , Issue 1. Pag: 270-279 consultado el 28 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/780000/771185/p270-neubauer.pdf?key1=771185&key2=2865207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Nuñez, A. (febrero, 2005) Estándares de seguridad de la información. UNAM. Consultado el 2 de marzo de 2005 en: http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

Pedemonte, S. (2005) CRM: El foco en sus Clientes más Valiosos. *ABC formación.* Consultado el 3 de junio del 2005 de: http://www.abcformacion.com/contenidos/calidad_0009.htm

Ramos M. (2003, feb 06) La seguridad informática, una ventaja competitiva según las entidades financieras. *Virus Prot.com.* consultado el 10 de octubre del 2004 de: http://www.virusprot.com/Nt060241.html

Roberts D. (diciembre 2, 2002) tif.: Viruses cost major IT users GBP122,000 per incident; Vendor independent study highlights need for better protection. *ACM Press, New York, NY, USA (diciembre 2, 2003) M2 Communications Ltd* consultado el 30 de enero del 2005 de: http://0-proquest.umi.com.millenium.itesm.mx/pqdlink?index=0&did=471686391&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1107118878&clientId=23693

Ruíz, J. (2004) Mexico Channel Manager consultado el 5 noviembre del 2004 de: http://www.afina.com.mx/download/ docs/iss/Presentacion%20ISS.ppt

Schechter S. y Smith M. (2003) Access for sale: a new class of worm. *ACM Press New York, NY, USA (2003).* SESSION: Internet WORMS: past, present, and future. Pag:19-23 consultado el 28 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/570000/566494/p7-neumann.pdf?key1=566494&key2=5914207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Servín, A. (2004). Diseño e implementación de algoritmo para la detección proactiva de falla de redes empresariales de datos. ITESM

Singh P. y Lakhotia (febrero, 2002) Analysis and detection of computer viruses and worms: an annotated bibliography. *ACM Press, New York, NY, USA (febrero, 2002)* Volume 37 , Issue 2 Pag. 29-35 consultado el 2 de noviembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/570000/568608/p29-singh.pdf?key1=568608&key2=0080640011&coll=portal&dl=ACM&CFID=31150506&CFTOKEN=33895484

Snyder L. (2003). Expanding Help Desk Services: The Benefits of Student S.O.S.
ACM Press New York, NY, USA (2003). Association for Computing Machinery. Pag: 74 - 79 consultado el 30 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/950000/947490/p74-snyder.pdf?key1=947490&key2=3255207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Stallings, W. (1996). Networking Standars, A guide to OSI, ISDN, LAN and MAN
standards. Sexta Edición, 1996. Addison Wesley

Tevis J. y Hamilton J. (2004) Methods for the prevention, detection and removal of software security vulnerabilities. *ACM Press New York, NY, USA (2004).* SESSION: Security. Pag: 197 - 202 consultado el 5 de octubre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/990000/986583/p197-tevis.pdf?key1=986583&key2=5842207901&coll=portal&dl=ACM&CFID=28897295&CFTOKEN=55602418

Toyoizumi H. y Kara A. (2002). Predators: good will mobile codes combat against computer viruses. *ACM Press New York, NY, USA (2002).* SESSION: Intrusion detection and response. Pag: 11 - 17 consultado el 28 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/850000/844105/p11-toyoizumi.pdf?key1=844105&key2=3906207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Weaver N., Paxson V. y Staniford S., Cunningham R. (2003) A Taxonomy of Computer Worms. *ACM Press New York, NY, USA (2003).* SESSION: Internet WORMS: past, present, and future. Pag: 11-18 consultado el 5 de octubre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/950000/948190/p11-weaver.pdf?key1=948190&key2=7164207901&coll=portal&dl=ACM&CFID=28621242&CFTOKEN=66221055

Weaver N., Hamadeh I., Kesidis G. y Paxson V. (2004) Preliminary results using scale-down to explore worm dynamics. *ACM Press, New York, NY, USA (octubre, 2004)* SESSION: Session 3, Pag. 65-72 consultado el 5 noviembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/1030000/1029628/p65-weaver.pdf?key1=1029628&key2=3041640011&coll=portal&dl=ACM&CFID=31150506&CFTOKEN=33895484

Zou C., Gong W. y Towsley D. (2002) Code Red Worm Propagation Modeling and Analysis *ACM Press New York, NY, USA (2002).* SESSION: Network security. Pag: 138-147 consultado el 28 de septiembre del 2004 de: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/590000/586130/p138-zou.pdf?key1=586130&key2=3230207901&coll=portal&dl=ACM&CFID=28897295&CFTOKEN=55602418

Sitios WWW (World Wide Web)

Center for Internet Security – Standards *CIS Home Page* consultado el noviembre 5, 2004 en: http://www.cisecurity.org/sub_form.html

CERT Coordination Center. *Carnegie Mellon University* consultado el octubre 30, 2004 en: http://www.cert.org/

Cisco System. *Cisco System Home Page* consultado el octubre 28, 2004 en: http://www.cisco.com

Corporación Universitaria para el Desarrollo de Internet A. C. *CUDI* consultado el 1 noviembre, 2004 en: http://www.cudi.edu.mx/

Computer Associates
http://www.ca.com/

Computer Security Institute. *CSI* consultado el octubre 28, 2004 en: http://www.gocsi.com/

Consultora afina
www.afina.com.mx/download/ docs/iss/Presentacion%20ISS.ppt

Consultora b-secure
http://www.bsecuregroup.com/

Consultora Marsh
http://www.marshriskconsulting.com/st/PDEv_C_370_NR_306_PI_263728.htm

Consultora Mancera
http://www.universia.net.mx/index.php/news_user/content/view/full/16463/

Consultora Profit de España
http://www.profit.es/21recdes.html

Diccionario de economía y finanzas
http://www.eumed.net/cursecon/dic/c13.htm

Director CETI UC. Tomado de la Revista Gerencia en Costa Rica
http://www.gerencia.cl/articulo.mv?sec=11&num=79&mag=1&wmag=

Distributed Intrusion Detection System, *DShield.org* consultado el octubre 30, 2004 en:
http://www.dshield.org/

Ebusinessforum de Grecia.
http://www.ebusinessforum.gr/content/downloads/Douligeris_SECURITYevent1.pdf

Glosario de términos de Disaster Recovery Planning (DRP)
http://www.albionresearch.com/disaster/glossary.php

IEEE *Xplore, IEEE* consultado el noviembre 4, 2004 en:
http://ieeexplore.ieee.org/Xplore/DynWel.jsp
Insecure.Org - Nmap Free Security Scanner, Tools & Hacking resources
Insecure.org Home Page consultado el noviembre 1, 2004 en:
http://www.insecure.org

Institute - Computer Security Education and Information Security Training.
The SANS Institute consultado el octubre 28, 2004 en: http://www.sans.org/

Internet Security Systems - Current Internet Threat Level *Internet Security Systems* consultado el octubre 28, 2004 en:
https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp

Ips en Linux el proyecto Charon
http://www.ecs.utdallas.edu/ACE/pdf/charon_2005.pdf

Microsoft Network Access Protection
http://www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx

Netreg Artículo digital consultado el día 30 de junio de 2005:
http://www.netreg.org/contrib/

Network Admission Control (NAC)
http://www.cisco.com/en/US/netsol/ns466/networking_solutions_sub_solution_home.html

Removedor de malware Microsoft.
http://www.microsoft.com/security/malwareremove/default.mspx

ResNetReg at Saint Mary's College. Saint Mary's College. Artículo digital consultado el día 11 de agosto de 2005:
http://www.saintmarys.edu/~hideg/netreg/

Security/Privacy Tools,Trojan,Spyware,Popup blockers & Fraud Protection, *Doshelp.com* consultado el noviembre 4, 2004 en: http://www.doshelp.com/

SecurityFocus . *SecurityFocus Home Page* consultado el octubre 30, 2004 en:
http://www.securityfocus.org/

Segmentación de red. Trend Micro. Artículo consultado el 25 de mayo del 2005 en:
http://www.trendmicro.com.cn/partner-web/tm_cisco/images/Designing%20Security%20Domains%20to%20Manage%20Outbreak%20Risk%20White%20Paper.pdf

Sociedad Latinoamericana para la calidad.
http://www.calidad.org/s/costo.pdf

Symantec Security Response, *Symantec Home Page* consultado el noviembre 4, 2004 en:
http://www.symantec.com/avcenter/index.html
Symantec en la Región de Latinoamérica
http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1261.html

TrendMicro. Firma de antivirus
http://www.trendmicro.com/la/home/enterprise.htm

The network Registration System. NorthWestern University. Artículo digital consultado el día 9 de agosto de 2005:
http://www.resnet.northwestern.edu/training/2002/winter/

Universidad de California Berkeley, página de políticas de seguridad.
http://security.berkeley.edu:2002/IT.sec.policy.html

Universidad Nacional de Colombia, lecciones sobre una política de seguridad.
http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Cap2-Politicas.html

Unix México
http://www.unixmexico.org/modules.php?name=News&file=article&sid=1148

Virus Alerts. *Microsoft TechNet Security Virus Alerts*. consultado el octubre 28, 2004 en: http://www.microsoft.com/technet/security/alerts/default.mspx

W32/Bropia MSN Messenger worm pollo en bikini. Trend Micro. Consultado el 30 de mayo del 2005 de:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FBROPIA%2EF&VSect=P

Wikipedia
http://es.wikipedia.org/wiki/Portada