



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED PÚBLICA QUE CONTIENE UN SERVIDOR WEB

Elder Alexander Prado Herrera

Asesorado por el Ing. Pedro Pablo Hernández Ramírez

Guatemala, mayo de 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED
PÚBLICA QUE CONTIENE UN SERVIDOR WEB**

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

ELDER ALEXANDER PRADO HERRERA

ASESORADO POR EL ING. PEDRO PABLO HERNÁNDEZ RAMÍREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, MAYO DE 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympto Paíz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympto Paíz Recinos
EXAMINADOR	Ing. Juan Alvaro Díaz Ardavin
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
EXAMINADOR	Ing. José Ricardo Morales Prado
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED PÚBLICA QUE CONTIENE UN SERVIDOR WEB

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha enero de 2011.

Elder Alexander Prado Herrera

Universidad de San Carlos de Guatemala



Facultad de Ingeniería
Escuela de Ciencias y Sistemas

Guatemala, 30 de enero de 2011

Ingeniero

Carlos Alfredo Azurdia Morales

Coordinador de Privados y Trabajo de Graduación

Respetable Ingeniero Azurdia:

Por este medio le informo como asesor del trabajo de graduación del estudiante universitario de la carrera de Ingeniería en Ciencias y Sistemas, ELDER ALEXANDER PRADO HERRERA, carné 200611078, que he revisado el trabajo de graduación titulado: "LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED PÚBLICA QUE CONTIENE UN SERVIDOR WEB", y a mi criterio el mismo está completo y cumple con los objetivos propuestos para su desarrollo según el protocolo.

Agradeciendo su atención a la presente,

Atentamente,

Ing. Pedro Pablo Hernández Ramírez
Asesor de trabajo de graduación
Colegiado: 7240

Pedro Pablo Hernández Ramírez
Ingeniero en Ciencias y Sistemas
Colegiado 7240



Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 29 de Septiembre de 2011

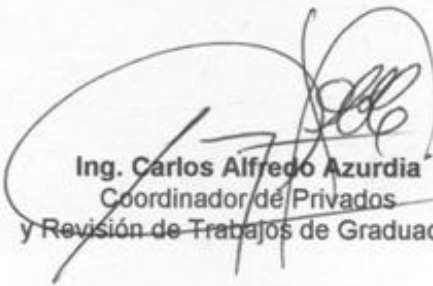
Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **ELDER ALEXANDER PRADO HERRERA** carné 2006-11078, titulado: **"LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED PÚBLICA QUE CONTIENE UN SERVIDOR WEB"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,


Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación



E
S
C
U
E
L
A

D
E

C
I
E
N
C
I
A
S

Y

S
I
S
T
E
M
A
S

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

*El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado **“LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED PÚBLICA QUE CONTIENE UN SERVIDOR WEB”** presentado por el estudiante ELDER ALEXANDER PRADO HERRERA, aprueba el presente trabajo y solicita la autorización del mismo.*

“ID Y ENSEÑAD A TODOS”

Ing. Marlon Antonio Pérez Turk
Director, Escuela de Ingeniería en Ciencias y Sistemas



Guatemala, 08 de mayo 2012



El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **LINEAMIENTOS PARA IDENTIFICAR VULNERABILIDADES EN UNA RED PÚBLICA QUE CONTIENE UN SERVIDOR WEB**, presentado por el estudiante universitario **Elder Alexander Prado Herrera**, autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olimpo Paiz Recinos
DECANO

Guatemala, Mayo de 2012



/cc
c.c. archivo.

ACTO QUE DEDICO A:

Dios	Por ser la fuente de mi inspiración y estar a mi lado en cada momento, dándome fuerzas para seguir adelante siempre y nunca darme por vencido.
Mis padres	Por creer siempre en mí, enseñarme los principios y valores que son fundamentales para alcanzar mis metas, además de su amor y cariño que me brindan día a día.
Mis hermanos y hermanas	Por darme su apoyo en todo momento y hacerme sentir su presencia y amor.
Mis padrinos	Por brindarme en todo momento su cariño y compartir muchos momentos de mi vida.
Mis amigos y amigas	Por permitirme compartir junto a ellos momentos inolvidables que siempre tendré presentes, y por tener el honor de convivir con ellos como hermanos.
Mis catedráticos	Por todas sus enseñanzas que son el cimiento del conocimiento de muchos profesionales y el mío.

**Universidad de
San Carlos
de Guatemala**

Por ser la casa de estudios donde logré alcanzar mi sueño de ser un profesional de bien para mi país, y enseñarme una nueva forma de vida.

**Todas las personas
que forman parte
de mi vida**

A quienes que por algún motivo hemos cruzado caminos o palabras, gracias por estar ahí; de todas aprendí algo muy valioso.

AGRADECIMIENTOS A:

**Universidad de
San Carlos de
Guatemala**

Por ser el centro donde pude desarrollar todos mis conocimientos, y culminar mi carrera.

**Ing. Pedro Pablo
Hernández Ramírez**

Por apoyarme en la realización de este trabajo de graduación, por guiarme en su desarrollo, motivándome a la realización de un buen trabajo.

**Ing. Luis Fernando
Espino Barrios**

Por ser el tutor en el desarrollo de este trabajo de graduación, brindándome los lineamientos para lograr finalizarlo.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES.....	VII
GLOSARIO	IX
RESUMEN.....	XIII
OBJETIVOS.....	XV
INTRODUCCIÓN	XVII
1. PRINCIPIOS BÁSICOS DE SEGURIDAD.....	1
1.1. Sistema de seguridad	3
1.2. Niveles de seguridad	4
1.2.1. Seguridad física	4
1.2.2. Protección del <i>hardware</i>	5
1.2.2.1. Desastres naturales	6
1.2.2.2. Desastres de entorno	6
1.2.2.3. Protección de datos.....	7
1.2.3. Seguridad lógica	7
1.2.3.1. Seguridad de usuario	7
1.2.3.2. Seguridad de red.....	8
1.2.3.3. Seguridad de aplicación	8
1.2.3.4. Seguridad de sistema operativo	8
1.3. Componentes de seguridad.....	8
1.3.1. Autenticación.....	9
1.3.2. Confidencialidad.....	9
1.3.3. No repudio.....	10
1.3.4. Autorización	10
1.3.5. Integridad	10

1.3.6.	Auditoría	11
1.3.7.	Disponibilidad	11
2.	LEGISLACIÓN – SEGURIDAD INFORMÁTICA	13
2.1.	Delitos informáticos	13
2.1.1.	Conceptualización	14
2.1.2.	Delitos informáticos definidos por la ONU	15
2.1.3.	Las Naciones Unidas y los delitos informáticos	16
2.1.3.1.	Fraudes cometidos mediante manipulación de computadoras.	17
2.1.3.2.	Falsificaciones informáticas	18
2.1.3.3.	Daños o modificaciones de programas o datos computarizados.....	19
2.2.	Legislación de Cyber-Crimen en Guatemala.....	22
2.2.1.	Situación actual	22
3.	ANÁLISIS DE RIESGOS Y VULNERABILIDADES.....	31
3.1.	Administración de riesgos.....	31
3.1.1.	Importancia de la administración de riesgos.....	32
3.1.2.	Metodología para valoración de riesgos	34
3.1.2.1.	Caracterización del sistema	34
3.1.2.2.	Identificación de amenazas	34
3.1.2.3.	Identificación de vulnerabilidades	35
3.1.2.4.	Control de análisis	35
3.1.2.5.	Determinación de probabilidades.....	35
3.1.2.6.	Análisis de impacto	36
3.1.2.7.	Determinación de riesgos	37
3.1.2.8.	Recomendaciones de control.....	38
3.1.2.9.	Documentación de resultados.....	39

3.2.	Análisis de vulnerabilidades.....	39
3.2.1.	Identificación de amenazas.....	41
3.2.2.	Estadísticas del CERT – Datos históricos.....	44
3.3.	Herramientas para análisis	51
3.3.1.	Sandcat.....	52
3.3.2.	VisualRoute.....	52
3.3.3.	WebInspect	52
3.3.4.	Nikto.....	52
3.3.5.	XProbe2	53
3.3.6.	Watchfire´s AppScan	53
3.3.7.	Acunetix Web Vulnerability Scanner	53
3.3.8.	Codenomicon HTTP Test Tool.....	54
3.3.9.	SecurityMetrics Appliance.....	54
3.3.10.	Lightning Console	54
3.3.11.	SARA:	55
3.3.12.	Qualys Free Security Scans.....	55
3.3.13.	Qualys Guard.....	55
3.3.14.	Perímeter Check	55
3.3.15.	STAT Scanner.....	56
3.3.16.	Nessus Security Scanner.....	56
3.3.17.	Secure-Me.....	57
3.3.18.	SAIN.....	57
3.3.19.	NMap Network Mapper	57
3.3.20.	NetIQ Security Analyzer:.....	58
3.3.21.	Foundstone	58
3.3.22.	CERIAS Security Archive.....	58
3.3.23.	Internet Scanner.....	59
3.4.	Análisis interno.....	59
3.4.1.	Personal – insiders.....	60

3.5.	Análisis externo	65
3.5.1.	Vulnerabilidades identificadas	69
3.5.1.1.	Módulo de PHP My_eGallery (NIKTO)	69
3.5.1.2.	Método HTTP TRACE (NIKTO)	69
3.5.1.3.	Servicio RealVNC versión 4.0 (NMAP)	69
3.5.1.4.	Servidor Web Microsoft IIS 6.0 (NMAP).....	70
3.5.1.5.	Plataforma Dokeos 1.8.5	70
3.5.1.6.	Joomla 1.5	70
4.	REDUCCIÓN DE RIESGOS – APLICACIÓN DE POLÍTICAS DE SEGURIDAD.....	75
4.1.	Reducción de riesgos	75
4.1.1.	Opciones en la reducción de riesgos	75
4.1.1.1.	Priorizar acciones	79
4.1.1.2.	Evaluar recomendaciones y opciones de control	79
4.1.1.3.	Realizar análisis costo/beneficio	79
4.1.1.4.	Seleccionar controles.....	79
4.1.1.5.	Asignar responsabilidades.....	80
4.1.1.6.	Desarrollar plan de implementación de protección	80
4.1.1.7.	Implementación de controles seleccionados ..	80
4.2.	Políticas de seguridad	81
4.2.1.	Etapas en el desarrollo de una política de seguridad	83
4.2.1.1.	Fase de desarrollo	84
4.2.1.2.	Fase de implementación.....	84
4.2.1.3.	Fase de mantenimiento	85
4.2.1.4.	Fase de eliminación	85

4.3.	Soluciones de vulnerabilidades.....	86
4.3.1.	Apache.....	91
4.3.1.1.	Configuración de Apache.....	91
CONCLUSIONES		93
RECOMENDACIONES.....		95
BIBLIOGRAFÍA.....		97

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Diagrama costo/seguridad/riesgo	3
2.	Diagrama de flujo, metodología para valoración de riesgos	33
3.	Porcentaje de ataques	42
4.	Detalle de ataques	43
5.	Vulnerabilidades catalogadas	45
6.	Cantidad de publicaciones de vulnerabilidades	47
7.	Publicaciones 1988-2004.....	49
8.	Mapa de tipo de vulnerabilidades	50
9.	Porcentaje de intrusiones	60
10.	Punto de red vulnerable.....	62
11.	Uso del comando nslookup.....	63
12.	Información obtenida con VisualRoute2010	66
13.	Gráfico obtenido con Visual Route 2010.....	67
14.	Pantalla de la herramienta Acunetix	71
15.	Vulnerabilidad por medio del método GET	72
16.	Estrategia de reducción de riesgos.....	77
17.	Propuesta para implementación de controles.....	78
18.	Etapas en el desarrollo de una política de seguridad	83
19.	Propuesta de uso de zona desmilitarizada (DMZ)	87

TABLAS

I.	Nivel de probabilidades.....	36
II.	Vulnerabilidades catalogadas por CERT	44
III.	Publicaciones sobre vulnerabilidades	46
IV.	Reporte de publicaciones 1988-2004	48
V.	Tabla de análisis de puertos	68
VI.	Recomendaciones de seguridad inalámbrica	88

GLOSARIO

Ataque	Ataque a una red, a menudo aprovechando una vulnerabilidad del sistema; los <i>hackers</i> a menudo envían vulnerabilidades descubiertas y sus ataques, lo que aumenta la importancia de un escaneo periódico de seguridad.
Ataque de denegación de servicio (DoS)	Ataque de extrema gravedad que sobrecarga los servidores web y evita que los usuarios legítimos puedan acceder al sistema.
Bitácora	Registro de todo lo relativo al funcionamiento de un sistema. Colección de mensajes que constituye el historial del tráfico de mensaje.
Cracker	Es aquella persona que investiga la forma de bloquear protecciones hasta lograr su objetivo, con malas intenciones. Usan programas propios, tales como rutinas que desbloquean claves de acceso o generadores de números para que en forma aleatoria y ejecutada automáticamente, puedan lograr vulnerar claves de acceso de los sistemas.

Descifrado	Aprovechamiento malicioso de una red informática.
Descifrado por la fuerza bruta	Intento de adivinación de una contraseña, realizando todas las posibles combinaciones de letras o números.
Escáner de puerto	Programa que “llama” a cada puerto (un total de 65.535) para comprobar cuáles están abiertos para acceder a una red.
<i>Firewalls</i> (Cortafuegos)	Es un sistema de seguridad, que suele ser una combinación de <i>hardware</i> y <i>software</i> , que se utiliza para proteger una red de las amenazas externas procedentes de otra red, incluyendo a Internet.
<i>Hacker</i>	Es una persona dedicada a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía.
Ingeniería social	Manipulación de usuarios para obtener información confidencial como contraseñas.
NAT	(<i>NetBios Auditing Tool</i>) herramienta de auditoría que enumera a todas las máquinas.

NMAP	NMAP o exploración de red, es una herramienta de escaneo que localiza los dispositivos de la red.
NSLOOKUP	Herramienta que utiliza un nombre de <i>host</i> para encontrar su dirección IP correspondiente.
Parche	Programa escrito para resolver la vulnerabilidad de una aplicación o sistema.
<i>Ping</i>	Herramienta que comprueba la conectividad de la red.
Rutinas	De averiguación de contraseña; se le llama así al intento de registro en una red aventurando contraseñas continuamente, hasta que una de las que se haya propuesto sea la correcta.
<i>Traceroute</i>	Herramienta que localiza el desplazamiento de los datos por medio de la red.
<i>Whois</i>	Herramienta que permite acceder a directorios que contienen información personal de contacto, como los nombres de empresas o individuos.
Zona de transición	(DMZ) zona de seguridad media entre los cortafuegos internos y externos de una red

RESUMEN

El ser humano posee necesidades innatas a su persona y entre ellas se encuentra el término conocido como seguridad, que es una de las necesidades básicas que debe satisfacer en contexto de prevención de la vida y sus posesiones, y es en este sentido, en el que se involucra a los sistemas de información, que en la actualidad se han convertido en uno de los activos más importantes de los seres humanos, debido a que la mayoría de actividades cotidianas son realizadas por medio de estos sistemas.

Actualmente, la seguridad involucrada en las tecnologías de información y telecomunicaciones se encuentra directamente relacionada con las organizaciones, que son las que deben velar por brindar a sus clientes “sistemas seguros”; aunque en los últimos años existen muchos grupos que promueven la legislación para delitos informáticos, brindando una protección extra a los sistemas.

Hoy en día, las tecnologías de información y comunicaciones son una herramienta principal en el desarrollo de las organizaciones, manejando toda la información de estas, con base en esta situación, el usuario se plantea el siguiente cuestionamiento ¿nuestra información se encuentra realmente segura?

Actualmente, no existen sistemas completamente seguros, pero sí se puede aumentar la seguridad de estos a niveles aceptables, buscando las vulnerabilidades y los puntos de falla, para poder corregirlos.

Dentro de los sistemas de información es posible crear las mejores políticas de seguridad que existen en la actualidad, pero un punto importante que no debe ser descuidado, es el lado de los usuarios, que muchas veces son el punto de falla de la mayoría de sistemas.

Este trabajo de graduación buscará ayudar a las organizaciones a identificar vulnerabilidades dentro de su organización, con el objetivo de reducir los riesgos de posibles ataques, así como también de dar algunas recomendaciones sobre políticas de seguridad que deben ser aplicadas en cualquier sistema de información.

OBJETIVOS

General

Establecer los lineamientos generales mínimos necesarios para la identificación de vulnerabilidades en una red de datos para medir la seguridad, permitiendo al administrador obtener información del estado de su red y soluciones a riesgos encontrados, brindando políticas de seguridad necesarias para tener un nivel aceptable de seguridad dentro de la red.

Específicos

1. Establecer lineamientos para identificar al menos tres vulnerabilidades en un sistema web.
2. Mostrar tres delitos informáticos identificados por la Organización de Naciones Unidas.
3. Mostrar el uso de al menos dos herramientas para la detección de vulnerabilidades en una red.
4. Identificar el porcentaje de usuarios que tengan el perfil para ser posibles atacantes.
5. Brindar al menos tres políticas necesarias para la seguridad de una red.
6. Dar solución al menos a tres vulnerabilidades encontradas.

INTRODUCCIÓN

La seguridad en los sistemas informáticos cada vez es más necesaria; esto debido al crecimiento que tienen los delitos informáticos. En la actualidad la mayoría de organizaciones está trasladando sus sistemas a la nube, lo que la mayoría de ocasiones los hace presa fácil de sufrir ataques.

Actualmente cualquier persona que lo desee puede tener acceso a lo que se conoce como internet, donde existe gran cantidad de información, que de estructurarse y seleccionarse de manera correcta, podría convertir a cualquier individuo en un potencial atacante.

En el siguiente trabajo de graduación se realiza una investigación acerca de los temas relacionados con la seguridad en los sistemas, enfocándose en el estudio de los sistemas web.

El primer capítulo contiene los conceptos fundamentales que deben conocerse por todas aquellas personas encargadas de la seguridad; están definidos los conceptos claves que conforman la seguridad en un sistema de TI; además, contiene una división por niveles para el estudio de las vulnerabilidades en los sistemas de TI y cómo prevenirlas.

En el desarrollo del segundo capítulo son estudiados los delitos informáticos, se dan a conocer los conceptos claves, y la clasificación que ha realizado sobre estos la Organización de Naciones Unidas (ONU). En Guatemala, al igual que muchos otros países, se están realizando legislaciones que penalicen a los cibercriminales, debido a esto existe una iniciativa de ley que es analizada para su pronta aprobación.

En el desarrollo del tercer capítulo, se muestran los pasos de una metodología para realizar el análisis de riesgos de cualquier sistema de TI; además se muestra un listado de posibles herramientas que pueden ser utilizadas para la detección de las vulnerabilidades del sistema, dichas herramientas deben ser utilizadas por los administradores de red para detectar y corregir vulnerabilidades; sin embargo, estas son utilizadas por los *hackers* para reconocer las vulnerabilidades y explotarlas. Con base en el análisis de algunas de estas herramientas, se realizaron pruebas y detectaron vulnerabilidades, que comúnmente se encuentran en la mayoría de sitios web.

El capítulo final, muestra una serie de pasos para la aplicación de políticas de seguridad que permitan reducir los riesgos y las amenazas, también se muestran soluciones a determinadas vulnerabilidades encontradas en la fase de detección de vulnerabilidades.

1. PRINCIPIOS BÁSICOS DE SEGURIDAD

Antes de iniciar el tema de seguridad, es relevante hacer énfasis sobre los aspectos que esta realmente abarca y sobre lo que significa. Actualmente, existen diferentes puntos de vista en que puede ser abordado. Uno de ellos, indica que es la forma de evitar pérdidas mediante la gestión de riesgos relacionados con la tecnología.

Haciendo una definición más formal en el ámbito de los sistemas computacionales: es la protección de los atributos de seguridad (integridad, disponibilidad, confidencialidad) sobre la información y todos los recursos que son utilizados por éstos sistemas.

Según el Departamento de Comercio del Instituto Nacional de Estándares y Tecnología (NIST); existe una serie de compromisos básicos que deben cumplir los sistemas de seguridad computacionales, estos son:

- No dificultar las labores de los usuarios: se refiere a que el sistema de seguridad, no debe intervenir en las funciones y acciones de los usuarios, es decir, debe ser transparente para este, siempre y cuando estén protegidos los recursos que son considerados como importantes.
- La seguridad es responsabilidad de la gestión de riesgos: se refiere a que en las organizaciones, el aspecto de seguridad debe ser tratado por un departamento o persona responsable, que será el encargado de administrar los riesgos.

- Las responsabilidades de seguridad deben ser especificadas: se refiere a que debe existir una delegación de responsabilidades y encargados de la supervisión para las diferentes áreas, que serán cubiertas por el sistema de seguridad.
- La estructura de seguridad debe ser clara: se refiere, que todo lo relacionado con la seguridad sea entendible para todos aquellos que de alguna manera estén involucrados en este contexto, para evitar que existan ambigüedades entre las responsabilidades, acciones e interacciones entre los elementos participantes.
- El costo de la protección del sistema debe ser aceptable: para toda organización, el costo de inversión que se utilice para implementar un sistema de seguridad tiene que estar relacionado con el valor de lo que se desea asegurar, esto porque no se puede gastar tanto en un sistema cuando lo que se desea proteger tiene un valor menor que el propio sistema de seguridad, en relación con el costo/beneficio; esto se puede apreciar más fácilmente en la siguiente desigualdad:

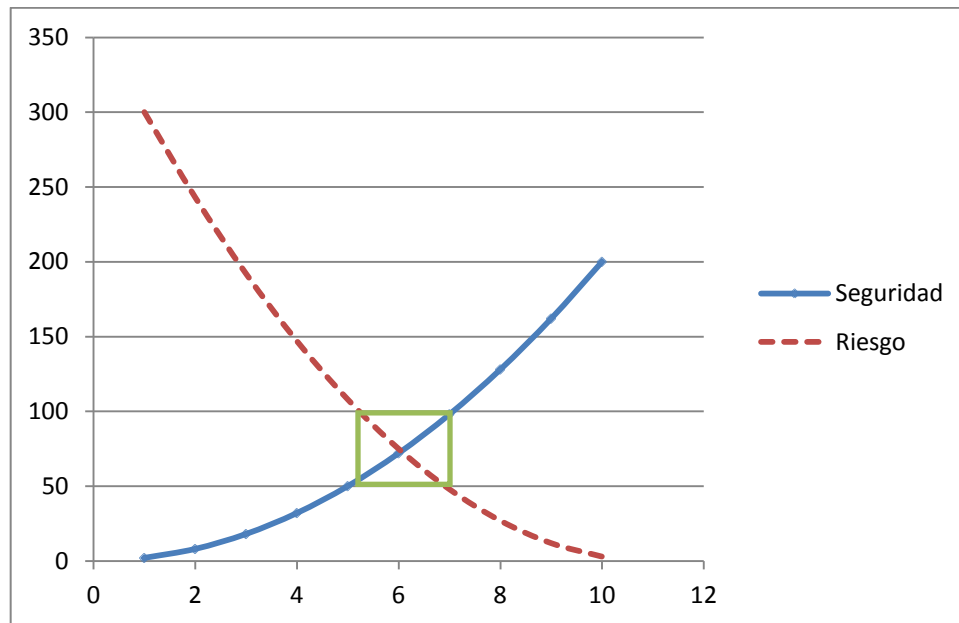
$$CH > CB > CS$$

CB: costo de los bienes que se desean proteger.

CS: costo del sistema de seguridad implementado.

CH: costo necesario para romper las medidas de seguridad.

Figura 1. **Diagrama costo/seguridad/riesgo**



Fuente: elaboración propia.

En la figura 1, el recuadro muestra el área de equilibrio en la cual se manejan estas tres variables.

1.1. **Sistema de seguridad**

Se conoce como sistema de seguridad al conjunto de elementos, tanto lógicos como físicos, que tiene como objetivo prevenir, evitar o reducir riesgos que puedan presentarse en determinadas circunstancias. Una de sus características más importantes es que es proactivo, para poder cubrir la mayor cantidad de vulnerabilidades posibles. Un sistema de seguridad óptimo puede brindar el soporte necesario en las organizaciones, minimizando las tareas de corrección y recuperación.

Un aspecto muy importante, que se debe tener en cuenta al hablar de un sistema de seguridad, es que se debe poseer algo que se desee proteger, y es en este sentido, cuando se realiza una clasificación de todos los elementos que contiene la organización, para determinar aquellos que necesiten ser protegidos, y la prioridad de la protección que debe ser establecida.

1.2. Niveles de seguridad

Un sistema de seguridad, debe manejar varios aspectos importantes, con los cuales pueda tener una buena valoración en las evaluaciones para medir el nivel de aseguramiento de los elementos que se estén protegiendo.

1.2.1. Seguridad física

Este nivel es uno de los más olvidados y se puede catalogar entre los más importantes; la mayoría de las veces, las empresas invierten considerablemente en sistemas informáticos, con el propósito de prevenir ataques externos como *hackers*, virus, etc. Todo esto es necesario la mayoría de veces, pero no se debe descuidar por ningún motivo cuestiones como, qué personas tienen acceso a los servidores o bien las estrategias que deben utilizarse en caso de algún suceso no esperado, como los fenómenos naturales.

En este nivel se debe garantizar, al igual que la seguridad externa, que cualquier *hacker* acceda a elementos protegidos, que ninguna persona no autorizada tenga acceso a estos elementos físicamente.

A nivel de seguridad física se define como: la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial.

1.2.2. Protección del *hardware*

En la mayoría de casos, el *hardware* constituye uno de los activos con mayor costo para las organizaciones y garantizar su integridad es uno de los principales factores que debe cuidar los sistemas de seguridad. A continuación se describen conceptos fundamentales:

- Acceso físico: se refiere a todas las medidas de seguridad que son implementadas y serán inútiles, si cualquier persona puede acceder físicamente a las máquinas. El nivel físico debe garantizar la seguridad tanto de la red como de los sistemas conectados a ella.
- Prevención: para evitar esto, existen varios métodos disponibles actualmente, donde puede variar el factor precio; muchas veces el principal factor para inclinarse hacia una u otra tecnología, como ejemplo, analizadores de retina, videocámaras, tarjetas inteligentes o control de las llaves que abren determinada puerta; todos estos son formas de autenticación, que se verán posteriormente, pero también puede implementarse acciones tan elementales, como contar con un laboratorio y mantenerlo con llave siempre.

- Detección: si el tema anterior, por cualquier motivo es imposible implementarlo, se debe tener un mecanismo que informe sobre cualquier anomalía que esté sucediendo, pero a pesar de detectarlos siempre debe existir el monitoreo y control, para reducir el riesgo de que las notificaciones de los problemas se informen tarde.

1.2.2.1. Desastres naturales

En muchas organizaciones, este aspecto pasa inadvertido y al momento de ocurrir cualquier desastre, se dan cuenta que el sistema de seguridad no los cubre; son riesgos latentes, que están ahí pero nadie se preocupa por ellos. Entre estos aspectos que se deben tomar en cuenta están:

- Terremotos
- Tormentas eléctricas
- Inundaciones y humedad

1.2.2.2. Desastres de entorno

Son todas aquellas perturbaciones, que pueden ocurrir en el medio en el cual se desenvuelve cualquier sistema de seguridad y que si no se toman las medidas necesarias puede causar pérdidas en las organizaciones. Entre los elementos que se deben tomar en cuenta en el análisis de riesgos por desastre del entorno están:

- Electricidad
- Ruido eléctrico
- Incendios y humo
- Temperaturas extremas

1.2.2.3. Protección de datos

Al referirse a seguridad física, en este caso *hardware*, también se deben aplicar políticas de seguridad que permitan asegurar la información que está contenida en los equipos, para evitar que pueda ser alterada o extraviada:

- Interceptación
- *Backup*

1.2.3. Seguridad lógica

Después de analizar las posibles causas que puedan afectar a cualquier sistema desde el punto de vista de seguridad física, ahora se debe analizar desde el punto de vista lógico y es hacia donde están dirigidos la mayoría de ataques y la información.

1.2.3.1. Seguridad de usuario

Consiste en educar a los usuarios que utilizan el sistema, para evitar que estos brinden cualquier tipo de información acerca de la empresa a terceros, que a simple vista parece ser irrelevante, pero que crea vulnerabilidades, aumentando el riesgo de sufrir ataques (como ejemplo revelar el sistema operativo que se utiliza), este tipo de extracción de información se le conoce como ingeniería social.

La denominada ingeniería social es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían.

1.2.3.2. Seguridad de red

En este nivel, se debe tener un control restringido y restrictivo de todos los nodos que pertenecen a la red, monitoreando sus actividades, además de gestionar todos los puntos de red y aquellos que no estén en uso, deshabilitarlos, para evitar cualquier tipo de ataque proveniente de estos puntos, evitando accesos no autorizados.

1.2.3.3. Seguridad de aplicación

Este nivel indica que, cada una de las aplicaciones que son empleadas dentro de la organización, debe poseer sus propios mecanismos de seguridad en el manejo de los datos.

1.2.3.4. Seguridad de sistema operativo

Este nivel se basa en las configuraciones que se realizan sobre los sistemas operativos; se debe evitar el uso de las configuraciones por defecto, debido a que son conocidas por todos y hacen al sistema más vulnerable.

1.3. Componentes de seguridad

Todos los sistemas de seguridad, para poder funcionar de manera eficiente ante las amenazas, a las que se exponen los elementos de valor que conforman las organizaciones y garantizar la protección de estos, es necesario que dichos sistemas contengan los siguientes atributos para asegurar su calidad y de esta manera, brindar un aceptable nivel de seguridad a las organizaciones.

1.3.1. Autenticación

Se necesita de una identificación con el propósito de asegurar que la entidad es quien dice ser y no es falsa; este atributo de seguridad es utilizado por la mayoría de organizaciones, aunque su nivel de complejidad puede variar dependiendo de las necesidades de cada una de ellas.

Este atributo cuenta con una división, que está dado por la forma de identificarse, las cuales son: contraseñas, que se refiere a información que se conoce; *hard tokens*, que se refiere a elementos físicos que se tienen; biométricos, que abarcan todo lo concerniente a lo que hace únicos a los seres humanos; híbridos, que son la combinación de dos o más tecnologías para la autenticación.

1.3.2. Confidencialidad

Este atributo hace referencia a que los elementos o información de la organización puedan ser accedidos únicamente por entidades autorizadas.

Este elemento, al igual que el anterior, también posee división, dependiendo de los niveles de aislamiento que se quieran utilizar dentro de la organización, siendo estos: público, donde cualquier persona puede acceder a este tipo de información; privado, solo personas autorizadas pueden acceder a este tipo de información, aunque su valor no es tan alto; estrictamente confidencial, solo personal restringido puede acceder a este tipo de información, la pérdida o acceso de personas no autorizadas puede involucrar grandes pérdidas para la organización.

1.3.3. No repudio

Este atributo de seguridad, permite conocer con certeza, que el mensaje fue entregado de forma correcta o no al destinatario. En este concepto, también se involucra el concepto de las firmas digitales, para garantizar la integridad del mensaje.

La firma digital, es una secuencia de datos, resultado de aplicar un conjunto de algoritmos matemáticos a dicho documento. Estos algoritmos permiten ofrecer garantías de seguridad sobre el documento objeto de firma.

1.3.4. Autorización

Este atributo, es el encargado de controlar los accesos sobre los elementos, con el objetivo que únicamente puedan acceder a ellos las entidades que tienen permiso para hacerlo, evitando que puedan ser manipulados por otras entidades.

Acerca de este atributo, merece la pena mencionar que es recomendado aplicar el principio de menor privilegio, que se refiere a que un objeto únicamente debe acceder a todo aquello que necesite y solo lo que necesite, evitando así, que tenga accesos no autorizados a regiones de los sistemas.

1.3.5. Integridad

Este atributo indica que, solo las entidades autorizadas son las encargadas de modificar la información y además, se debe velar para que dentro de la información no existan ambigüedades, ni datos incorrectos.

1.3.6. Auditoría

Es la encargada de analizar y controlar que todas las operaciones queden registradas dentro del sistema, para poder identificar las causas de los errores, fallas y ataques dentro del sistema.

Este atributo también contiene una división, la cual se divide en: *post mortem* (después del crimen), como su nombre lo indica permite realizar un análisis luego de identificado y registrado un suceso; activo, el cual le permite al sistema detectar y responder a errores, fallas y ataques en el momento que suceden.

1.3.7. Disponibilidad

Se refiere a que los recursos del sistema se encuentren disponibles, para las entidades debidamente autorizadas, en el momento que estas los necesiten y no tengan que esperar por ello.

2. LEGISLACIÓN – SEGURIDAD INFORMÁTICA

2.1. Delitos informáticos

Actualmente, el cambio mundial que se está dando en las sociedades, por medio de las tecnologías de la información y comunicaciones, está ayudando a mejorar los procesos de las industrias, permitiéndoles innovar en sus áreas de producción y optimizando el uso de sus recursos; sin embargo, todo esto también trajo aspectos negativos, como todas las formas de delincuencia informática.

Este tipo de delincuencia, en la rama de la informática, es un área de la cual no se puede definir con certeza, debido a que la ciencia de la computación es un campo relativamente nuevo, donde aún se está descubriendo muchas de sus aplicaciones.

Con base en la legislación y/o la jurisprudencia, se le considera a la delincuencia informática, como una conducta proscrita, que implica el uso de las tecnologías de la información y comunicaciones para delinquir.

2.1.1. Conceptualización

Como se menciona anteriormente, no existe una definición dada por la Real Academia de la Lengua Española, pero a pesar de ello, muchos expertos en esta área, han formulado sus propios conceptos, tomando como punto de partida las situaciones por las que se han encontrado. En el ámbito internacional se considera que no existe una definición propia del delito informático, sin embargo al consultar la bibliografía internacional, específicamente al estudioso español Carlos Sarzana, en su obra Criminalidad e tecnología, los crímenes por computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

A continuación se muestran los criterios doctrinales de algunos tratadistas al respecto:

- Nidia Callegari define al "delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas".
- Rafael Fernández Calvo define al "delito Informático" como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española.

- María de la Luz Lima dice que el "delito electrónico", "en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".
- Julio Téllez Valdés conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

2.1.2. Delitos informáticos definidos por la ONU

El avance de las tecnologías de la información y las comunicaciones, no solo ha significado avances beneficiosos, también existen avances en los delitos informáticos y lo más preocupante, que cada vez son realizados con mayor frecuencia, debido a estos acontecimientos, la mayoría de países se han visto influenciados a promover y modificar sus legislaciones en contra de los delitos informáticos, con el objetivo de poder erradicarlos.

Sin embargo, a pesar que es un fenómeno que está afectando a todo el mundo, al momento de establecer las leyes en contra de este tipo de delitos, se encuentra de que es necesaria la cooperación de todos los países para que dichas legislaciones no violen estos derechos; esto tiene ciertas complicaciones ya que es fácil encontrar incompatibilidades entre las legislaciones de una y otra nación.

Actualmente, se están desarrollando diversas iniciativas que buscan promover la cooperación internacional y hacer conciencia sobre la lucha contra los delitos informáticos.

2.1.3. Las Naciones Unidas y los delitos informáticos

El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los problemas y las insuficiencias; por cuanto, los delitos informáticos constituyen una forma de crimen transnacional y su combate requiere de una eficaz cooperación concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición de dichas conductas delictivas.
- Falta de especialización en las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de las computadoras.

- Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

2.1.3.1. Fraudes cometidos mediante manipulación de computadoras

- Manipulación de los datos de entrada: este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común debido a que es fácil de cometer y difícil de descubrir.
- Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
- Manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático, para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora, en la fase de adquisición de datos. Tradicionalmente, esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados, para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las de crédito.
- Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo: es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2.1.3.2. Falsificaciones informáticas

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas.

- Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos, e incluso crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

2.1.3.3. Daños o modificaciones de programas o datos computarizados

- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización, funciones o datos de computadora, con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
 - Virus: es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
 - Gusanos: se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos; pero es diferente del virus porque no puede regenerarse.

En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá, puede

dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- Bomba lógica o cronológica: exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al contrario de los virus o gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
- Acceso no autorizado a servicios y sistemas informáticos: puede darse por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (*hackers*) hasta el sabotaje o espionaje informático.
- Piratas informáticos (*hackers*): el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden

emplear contraseñas comunes o de mantenimiento, que están en el propio sistema.

- Reproducción no autorizada de programas informáticos con derechos reservados: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales, con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Considerando, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

2.2. Legislación de Cibercrimen en Guatemala

Actualmente, el congreso de Guatemala está planteando una iniciativa de ley para el combate al cibercrimen. Esta involucra una reflexión y pensamiento acerca de cuál será el panorama en cuanto a cibercrimen o delitos cibernéticos en Guatemala, cuál es su posición o participación a nivel mundial sobre este aspecto, cómo es visto el país por otros países y qué medidas son o han sido implementadas sin la existencia de esta ley, a casos o problemas presentados en el país relacionados con el tema.

2.2.1. Situación actual

El documento se encuentra descrito o nombrado como iniciativa, que dispone aprobar una ley contra cibercrimen, por lo que se espera que este plantee las bases sobre las cuales se debe fundamentar en Guatemala, además de impulsar la aprobación de la misma por medio de justificación de la necesidad de su existencia.

El documento plantea un aspecto importante que se debe tomar en cuenta, que parece estar bien fundamentado, aunque de cierta manera generaliza un poco respecto de tal idea, describiendo el comportamiento o evolución en el comportamiento de una persona que se dedica al área de informática y consigue obtener conocimientos de acceso no autorizado como lo describe el texto “Del ansia del saber al ansia de poseer”.

De esta manera, describe la evolución en la pérdida de valores de la persona que inicia sus conocimientos con el fin de conocer, aprender o formarse en una rama de la informática, al punto de buscar, robar información, suplantar a una persona, robar dinero y realizar ataques, aunque su fin no sea mostrar vulnerabilidades en sus sistemas a las empresas y/o personas encargadas de una red o servicio en internet.

El texto clasifica o etiqueta a estas entidades como agresores o delincuentes de hecho; hace la comparación de personas que hace una década se dedicaban a este tipo de actividades, nombrándolos como agresores pero los describe como personas que tienen por fin aprender e investigar y ayudar a describir vulnerabilidades que podían ser explotadas por alguien con otro tipo de fines, diferente al de aprender. Como según el texto es en la actualidad.

Hasta este punto la iniciativa de ley fundamenta sus argumentos en plantear la falta de seguridad en la informática, hace notar que la sofisticación de los ataques en la actualidad y la experiencia y conocimientos de los atacantes, no está bien generalizar; no se puede decir que todas las personas que realizan ataque o acceden de manera no autorizada a un servidor o red, definitivamente están realizando un acto delictivo en contra de la sociedad o ciudadanos, pero al ser tomada en cuenta esta iniciativa y en caso de ser aprobada, en relación con lo expuesto anteriormente, y la manera en que se plantea la situación, podría ser interpretado cualquier tipo de estas prácticas como un crimen cibernético.

No importando si la persona que realice dicho ataque únicamente lo haga como un ejercicio de aprendizaje y no diferenciando entre estos últimos o como el mismo texto lo indica, las personas que llevaban a cabo ataques como estos con fines de hacer notar vulnerabilidades, o únicamente para aprender y encasillándolos junto con lo que ellos llaman como crimen organizado cibernético, de tal manera que cualquiera que lleve a cabo un hecho de este tipo, sería tomado como un delincuente ante los ojos de la justicia, y por tanto debería de ser penado como tal; hablando en términos de lo planteado por la iniciativa de ley.

El texto menciona y hace notar cómo a partir del año 2002 el concepto de ciberdelincuencia cambió completamente; indica un incremento en los ataques que al ser cada vez más sofisticados, se vuelven mucho más difíciles de detectar. De aquí se vuelve necesario tomar en cuenta todo tipo de amenazas y esto es una justificación adecuada, pues la internet ya no es segura para hogares ni negocios; son requeridas medidas de seguridad avanzadas que no están al alcance de usuarios comunes o con recursos no tan elevados, también para las empresas, implica gastar en medidas de seguridad que requieren de un mantenimiento y monitoreo que implica costos, que en caso de haber una mejor regulación de los ataques a usuarios de la red, no sería necesario tomarlos en cuenta.

Al analizar los gastos y medidas que deben de ser implementadas en las empresas y hogares, para evitar ataques e infiltración así como acceso no autorizado, de igual manera la infección por *malware* del equipo, es fácil notar que una gran cantidad de dinero es invertido en protección debido a la poca o casi nula seguridad; este es dinero que podría ser utilizado de manera diferente para optimizar ganancias de una empresa o inclusive para otros fines en hogares y familias.

En otra sección de la iniciativa se plantea el problema de las *botnets*, se hace referencia al *malware* incorrectamente como virus y se le responsabiliza del contagio de los ordenadores que luego forman parte de las *botnets*; se hace un recorrido breve sobre el funcionamiento y los objetivos para los cuales son creadas dichas *botnets* y cómo son utilizadas para generar dinero en manera inadecuada, enviando correos de publicidad y convirtiendo a los ordenadores comunes y corrientes, en parte de un ejército de ordenadores atacantes; explica a grandes rasgos y hace ver cómo la falta de seguridad ha creado campo para que las personas o usuarios comunes se conviertan en una amenaza para empresas o inclusive otros usuarios de internet.

La iniciativa de ley hace ver la situación en que las *botnets* y el *software* utilizados para este tipo de actividad y cualquier otro tipo de actividades criminales cibernéticas, son considerados como no existentes dentro del país, hecho que según indica el documento no es así; existe una gran cantidad de compra y venta de *software* para este tipo de fines, situación alarmante, pues como indica el documento, no hay más impedimento que el precio del mismo producto.

Este es un buen fundamento, pues como se plantea al inicio, se esperaba que este documento diera una idea más acertada sobre cómo es visto a nivel internacional o cómo es tomada la actividad criminal cibernética llevada a cabo en Guatemala; esto demuestra que existe una gran cantidad de tráfico de *software* de este tipo y que puede ser visto el país a nivel internacional o por países con quienes guarda relación como un país generador.

Esto permite el tráfico de mercancía por así llamarla, que afecta la economía de dicho país o inclusive organizaciones o grupos de países, de tal manera que el no contar con una ley anticiberdelincuencia en Guatemala lo sitúa en una posición no amistosa en ese aspecto y hasta cierto punto podría ser considerado como hostil, por no tomar medidas y permitir transacciones generadoras de ataques e inestabilidad para empresas y gobiernos.

Desde este punto de vista, el no contar con una ley anticiberdelincuencia Guatemala estaría posicionándose en una situación de indiferencia, siendo más amigos de delincuentes que de países amigos con quienes lleva a cabo negociaciones y transacciones. Es por eso que no es de extrañar que países como Estados Unidos, ejerzan medidas de presión sobre países que no están afiliados a una normativa para el tráfico y moderación de accesos y ataques no autorizados, para que de esta manera, dificultar más el tráfico de *software* creado con intenciones de suplantación, robos y ataques, así como desestabilización.

Esta iniciativa arroja luz y justifica correctamente los motivos por los cuales cada vez se hace más necesario formar parte para un país de un compromiso, tanto para sus habitantes y empresas, como para otros países y su protección y seguridad, pensando dentro de sí mismo las actividades inadecuadas y no autorizadas en la web, previniendo de esta manera y sentando reglas y normas a seguir, esto debería en teoría frenar el tráfico de *software* no autorizado o con fines de daño robo o suplantación; esto de hecho se mejoraría la imagen de Guatemala a nivel internacional; una iniciativa de ley mejoraría grandemente o al menos arreglaría la forma en que es visto el país en el exterior y tal vez, hasta cierto punto, sus relaciones con países amigos.

El documento en cuestión expone una gran cantidad de tipos de *malware* explicando la finalidad de cada uno y cómo afecta a usuarios o empresas; realmente es necesario exponer claramente el funcionamiento y fin de cada *software* malicioso existente para tener una adecuada y consistente justificación de una ley y normas como esta.

Expone también una línea de crecimiento en cuanto a agresividad y complejidad del *malware*, concepto que hace notar que algo que parecía ser pruebas inofensivas y ataques pequeños, en poco tiempo evolucionó a grandes ataques y estrategias de ataques para crimen esto hace notar que de no ser tomada una medida pronto, se estaría ante un panorama probablemente de formas de ataques mucho mejor organizados, más agresivos y mucho más dañinos para la sociedad, clientes de internet tanto usuarios como empresas y a todo tipo de redes inclusive para naciones o regiones grandes.

De no tomarse una medida en el tiempo adecuado y justo, lo antes posible, Guatemala o países que no colaboren con proponer, poner en práctica y evolucionar en técnicas para prevenir el cibercrimen dentro de su región, podrían verse envueltos en problemas mayores y de mayor responsabilidad, y probablemente enfrentar cargos serios por negligencia y por haber permitido durante tanto tiempo que dichas actividades se llevaran a cabo.

El propósito de este documento de iniciativa de ley es prevenir los cibercrímenes, y es parte de un movimiento o inicio de una norma tomada por países importantes, con el afán de disminuir la delincuencia cibernética, y si no se puede darle fin, al menos sentar precedentes que sean suficiente motivo para desmotivar y mantener al borde de la ley a personas que se dedican a este tipo de actividades.

La iniciativa de ley contra el cibercrimen en Guatemala, no es una idea propia ni nueva del país, es parte de un movimiento, de un esfuerzo para crear una ley uniforme que permita juzgar y penalizar a las personas que transgredan esta ley, de igual manera en cualquier parte del mundo y acá se ejemplifican las formas en que puede ser llevado a cabo un ataque, muestra la vulnerabilidad de un cliente o usuario ante cualquier aplicación, que podría ser una descarga de un archivo que el usuario desconoce que es un *malware*.

En el documento se refleja claramente un buen estudio del tema pues contiene información bastante técnica, que no es de conocimiento común, es decir no es conocimiento que el público tenga.

Define los tipos de ataques y detalla en qué consisten; describe qué es una vulnerabilidad y cómo es explotada por un agresor; en sí, resume qué es un ataque cibernético y por qué es considerado como tal, describiendo en parte el proceso de infección o qué lleva al ataque, cómo se desarrolla, o cuál es su fin.

También hace un rápido análisis de las tendencias que se espera según expertos, que tomarán los ataques y crímenes cibernéticos; esto podría brindar soporte para próximas modificaciones y actualizaciones de la ley, pues al estar sujeta a la tecnología que es cambiante, debería en teoría mantenerse al día de las modificaciones y cambios; también tendría que ser una ley que pueda ser fácilmente modificada y fácil de actualizar, según las nuevas amenazas o la evolución de las ya existentes.

Especifica también regiones por cantidad de cibercrímenes llevados a cabo y sugiere lo que se desea contener y controlar para que sea tomado en cuenta.

Luego de un intenso análisis, planteamiento de problemáticas y posibles soluciones así como el desglose de los tipos de ataques, cómo se llevan a cabo y cuáles son sus tendencias, la iniciativa de ley presenta de manera formal y legal cómo se espera que sea llevada a cabo y ejecutada dicha ley, y enumera todas y cada una de las actividades que son consideradas como ataques cibernéticos que deben ser penalizados.

Es importante hacer notar que la ley está sujeta a situaciones reales, que han sido conocidas por medio de problemas y ataques y experiencia sobre cómo se comportan en la actualidad los agresores y que debería ser una ley bastante flexible, para adaptarse a los cambios y tendencias tecnológicas y criminales, que probablemente necesitará una gran cantidad de tiempo para ser interpretada, llevada a cabo y ejecutada de forma efectiva, pues con el tiempo, una gran cantidad de nuevos tipos de ataques y tendencias podrían aparecer y el que esta ley no cubra dichos problemas, significará una gran pérdida o el ataque que podría quedar en la impunidad únicamente por la falta de actualización.

La iniciativa de ley parece enfocarse únicamente en cuatro áreas de posible crecimiento de crimen informático y deja cerradas a nuevas posibilidades, nuevos campos o técnicas criminales que por obvias razones no pueden ser predichas, hasta únicamente después de haber sucedido un percance de dicho tipo y luego de haber descifrado qué sucedió y haber aprendido la nueva técnica o tendencia, la iniciativa de ley por hoy es una excelente propuesta para prevenir y advertir, contener y penalizar a personas que se dediquen a cualquiera de las áreas comunes de ataque o donde mayor cantidad de atacantes se encuentren.

Dentro de la definición formal como ley de esta iniciativa hay un extenso vocabulario o grupo de definición de conceptos técnicos de informática que permiten analizar a personas que no cuentan con conocimientos amplios de *software* y *hardware*, de redes e internet, ni de *malware*, formarse un criterio; en general, es una buena propuesta, está bastante completa y resume en gran parte, de muy buena manera, lo más conveniente para el país y sus relaciones con países amigos.

Con la nueva norma mundial, se trabajará en armonía para evitar ser juzgado o visto como una nación que apoya los ataques recibidos por usuarios comunes, empresas, naciones o regiones y se mantendrá una mejor relación con el exterior, además de evitar posibles confrontaciones o responsabilidad grave en un ataque grande o verse implicado en problemas de mayor trascendencia.

3. ANÁLISIS DE RIESGOS Y VULNERABILIDADES

3.1. Administración de riesgos

La gestión de riesgos comprende tres procesos muy importantes, los cuales son: la evaluación, mitigación y la evaluación y valoración. Durante el proceso de evaluación de riesgos, se incluye la identificación y evaluación y los impactos, además la recomendación de medidas para la reducción de estos.

En la mitigación del riesgo, se refiere a dar prioridad, implementar y mantener las medidas apropiadas recomendadas durante el proceso de evaluación. Mediante el proceso de evaluación continua se brindan las claves para implementar un programa de gestión de riesgos con éxito.

El encargado de aprobar y autorizar esto, es responsable de determinar si el riesgo restante se encuentra en un nivel aceptable o si los controles de seguridad adicionales se deben implementar para reducir más, o eliminar el riesgo residual antes de autorizar (o acreditar) el sistema informático para la operación.

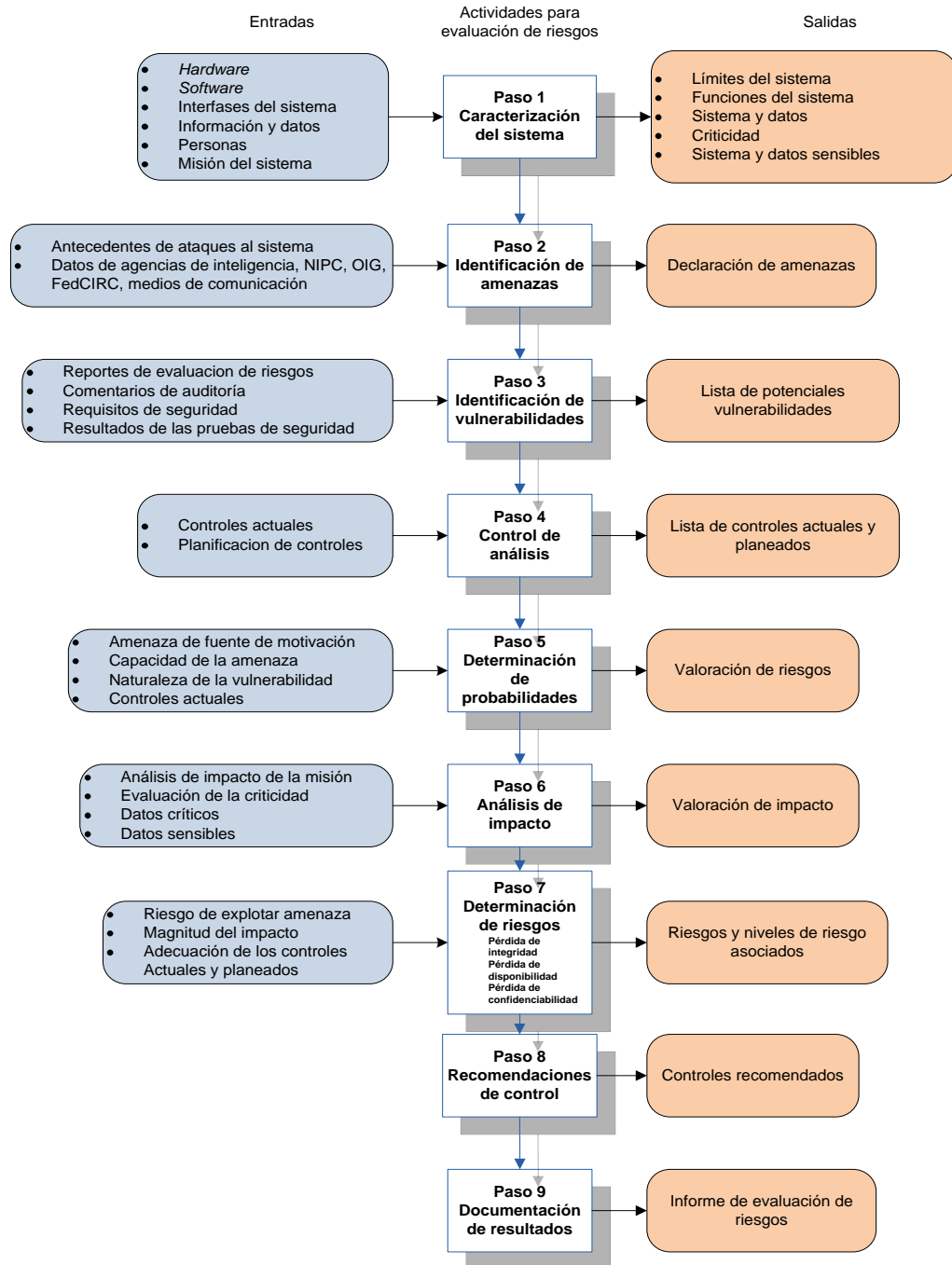
3.1.1. Importancia de la administración de riesgos

La gestión de riesgos es el proceso que permite a los administradores de TI, equilibrar los costos operativos y económicos de las medidas de protección, para conseguir mejoras en la capacidad de la misión de proteger los sistemas informáticos y los datos que apoyan las misiones de sus organizaciones. Este proceso no es exclusivo del entorno de TI y, de hecho que domina la toma de decisiones en todos los ámbitos de nuestra vida cotidiana.

El jefe de una unidad de organización debe asegurarse de que la organización tenga la capacidad necesaria para cumplir su misión. Estos administradores deben asegurar que la misión se cumpla, y determinar las capacidades de seguridad que sus sistemas de TI deben tener, para proporcionar el nivel deseado; logrando así hacer frente a las amenazas del mundo real.

La mayoría de las organizaciones tienen presupuestos limitados para la seguridad de TI, por lo tanto, el gasto de seguridad en TI debe ser revisado a fondo. Una metodología de gestión de riesgos bien estructurada y utilizada, puede ayudar a identificar los controles de gestión adecuados, para proporcionar las capacidades de seguridad esenciales y cumplir los objetivos de la organización.

Figura 2. Diagrama de flujo, metodología para valoración de riesgos



Fuente: elaboración propia.

3.1.2. Metodología para valoración de riesgos

Esta metodología es una serie de pasos para la correcta valoración de riesgos en un sistema informático, la cual puede detectar los puntos débiles del sistema para fortalecerlos y así reducir el número de vulnerabilidades.

3.1.2.1. Caracterización del sistema

Durante la fase de evaluación de riesgos para un sistema de TI, uno de los primeros pasos es definir el ámbito del esfuerzo. En este paso, se identifican los límites del sistema de TI, además de los recursos y la información que constituyen el sistema. La caracterización de un sistema de TI, establece que el ámbito del esfuerzo de evaluación de riesgos, delimita la autorización de funcionamiento (o acreditación), y proporciona la información esencial para definir el riesgo.

3.1.2.2. Identificación de amenazas

Una amenaza es la posibilidad de que un riesgo en particular, pueda afectar con éxito alguno de las vulnerabilidades con que cuentan las organizaciones. Una vulnerabilidad es una debilidad que puede ser accidentalmente disparada o explotada intencionalmente. Una amenaza no representa un riesgo cuando no existe una vulnerabilidad que para que pueda ser ejercida.

Para determinar la probabilidad de una amenaza, se debe considerar los riesgos, las posibles vulnerabilidades y los controles existentes.

3.1.2.3. Identificación de vulnerabilidades

El análisis de la amenaza a un sistema de TI debe incluir la identificación de las vulnerabilidades asociadas con el entorno del sistema. El objetivo de este paso es desarrollar una lista de las vulnerabilidades del sistema (fallas o debilidades) que podría ser aprovechada por amenazas potenciales.

3.1.2.4. Control de análisis

El objetivo de este paso es analizar los controles que se han implementado, o están próximos a ser implementados por la organización, para minimizar o eliminar la probabilidad de una amenaza de afectar una vulnerabilidad del sistema.

Para obtener una calificación de riesgo global que indique la probabilidad de que una vulnerabilidad potencial pueda afectar a la organización, la aplicación de los controles actuales y previstos deben ser considerados. Por ejemplo, una vulnerabilidad no es probable que afecte, o la probabilidad es baja si hay un bajo nivel de amenaza o bajo interés en afectarlo.

3.1.2.5. Determinación de probabilidades

Para obtener una calificación de riesgo global que indique la probabilidad de que una vulnerabilidad potencial puede afectar dentro del entorno de las amenazas asociadas, los siguientes factores de gobernabilidad deben ser considerados:

- Capacidad y motivación de amenaza
- La naturaleza de la vulnerabilidad

- Existencia y eficacia de los controles actuales

La probabilidad de que una vulnerabilidad potencial sea explotada por una amenaza concreta es descrita como alta, media o baja. La siguiente tabla describe estos tres niveles de probabilidad.

Tabla I. **Nivel de probabilidades**

Nivel de probabilidades	Definición de probabilidades
Alto	La amenaza es altamente motivada y lo suficientemente capaz, los controles para evitar esta vulnerabilidad están siendo ejercidos o son ineficientes.
Medio	La amenaza es altamente motivada y lo suficientemente capaz, pero los controles son capaces de impedir con éxito el ejercicio de la vulnerabilidad.
Bajo	La amenaza carece de motivación o no es lo suficientemente capaz y los controles evitan u obstaculizan de forma significativa el ejercicio de la vulnerabilidad.

Fuente: elaboración propia.

3.1.2.6. Análisis de impacto

Lo importante en este paso es la medición de nivel de riesgo y determinar los efectos adversos derivados de un ejercicio que amenaza tener éxito dentro de una vulnerabilidad. Para iniciar con esto es necesario contar con la siguiente información:

- Misión del sistema
- Datos críticos del sistema
- Datos sensibles del sistema

Esta información puede obtenerse a partir de la documentación existente dentro de la organización, tales como el informe de misión y el análisis del impacto o del informe de evaluación de la criticidad de los activos.

Un análisis de la misión prioriza los niveles de impacto asociados con el compromiso de los activos de información de una organización basada en una evaluación cualitativa o cuantitativa de la sensibilidad y criticidad de los activos.

Una evaluación de la criticidad de los activos identifica y da prioridad a los activos de la organización sensible y crítica de información, que apoyan las misiones fundamentales de la organización.

3.1.2.7. Determinación de riesgos

El propósito de este paso es evaluar el nivel de riesgo para el sistema de TI. La determinación del riesgo de una amenaza particular para una vulnerabilidad se puede expresar como una función de:

- La probabilidad de una amenaza concreta que pueda afectar una vulnerabilidad dada.
- La magnitud del impacto que puede ser una amenaza con éxito en el ejercicio de la vulnerabilidad.
- La adecuación de los controles de seguridad existentes o previstos para reducir o eliminar el riesgo.

3.1.2.8. Recomendaciones de control

Durante este paso, se proporcionan los controles que podrían mitigar o eliminar los riesgos identificados. El objetivo de los controles es reducir el nivel de riesgo para el sistema informático y sus datos a un nivel aceptable. Los siguientes factores deben ser considerados en la recomendación de los controles y las soluciones alternativas para minimizar o eliminar los riesgos identificados:

- Eficacia de las opciones recomendadas
- Legislación y reglamentación
- Organización política
- Impacto operacional
- Seguridad y fiabilidad

Las recomendaciones de control son los resultados del proceso de evaluación de riesgo y aportaciones al proceso de mitigación de riesgo, durante el cual los controles de seguridad recomendados de procedimiento y técnicos son evaluados, priorizados y ejecutados.

3.1.2.9. Documentación de resultados

Cuando la evaluación del riesgo se ha completado (amenazas y vulnerabilidades identificadas, las fuentes, los riesgos, y recomendación de controles), los resultados deben ser documentados en un informe oficial.

Un informe de evaluación de riesgos, es un documento de gestión que ayuda a la alta gerencia, los dueños de la misión, a tomar decisiones sobre la política, el presupuesto de procedimiento, y cambios en el sistema operacional y de gestión. A diferencia de un informe de auditoría o investigación, que busca la maldad, un informe de evaluación de riesgos no debe ser presentado en forma acusatoria, sino como un enfoque sistemático y analítico para la evaluación de riesgo, de manera que la alta gerencia entienda los riesgos y asigne recursos para reducir y corregir posibles pérdidas.

3.2. Análisis de vulnerabilidades

Con base en los niveles de seguridad, abordados con anterioridad, se puede relacionar con elementos que en la actualidad deben ser gestionados de una correcta manera, con el objetivo de minimizar el impacto que puedan tener los riesgos en materia de seguridad.

Un análisis de vulnerabilidades para un sistema de TI, no es más que otro sistema informático o red de sistemas que se encuentra relacionado con la terminología de seguridad para la detección e identificación de riesgos y vulnerabilidades que pueden ser explotadas por cualquier tipo de amenaza.

Un análisis de vulnerabilidades es utilizado para lograr que las medidas de seguridad implementadas o propuestas, sean las necesarias para proteger al sistema. Los *software* que brindan la posibilidad de detectar vulnerabilidades mediante escaneo, la mayoría de las veces no son utilizadas con propósitos de detección para proteger a los sistemas, sino que también, son utilizadas por los *hackers* para lograr penetrar e invadir el sistema; pero un administrador que utilice de correcta manera estos *software*, puede prevenir con eficacia la piratería y ataques en el futuro a su sistema.

Cuando se habla de análisis de vulnerabilidades, comúnmente se mencionan dos tipos de estrategia; la primera es la estrategia pasiva, que su nombre real es basado en *host*, esta se encuentra por encima del sistema en ambientes que no son los adecuados como mecanismos de contraseña débiles y conflictos entre políticas de seguridad. También existe la estrategia activa, o basada en red; esta encuentra las vulnerabilidades y por medio de los archivos de comandos registra el comportamiento del sistema, que haya detectado la vulnerabilidad.

Existen cuatro tipos de técnicas de escaneo para la detección de vulnerabilidades:

- Técnica de detección: consiste en una forma pasiva, que solo detecta y no elimina las vulnerabilidades encontradas dentro de un sistema.
- Detección de la tecnología basada en host: esta técnica al igual que la anterior utiliza la estrategia pasiva; generalmente implica el núcleo del sistema analizado, sus atributos, además de los parches y actualizaciones al sistema operativo. Esta técnica también provee un descifrado de

contraseñas fácil de eliminar. Esta técnica presenta desventajas dependiendo de la plataforma que se esté utilizando.

- Estrategia pasiva, comprueba las propiedades del sistema y archivos, como bases de datos y registros: la aplicación de esta tecnología su aplicación radica en ejecutar un ciclo cerrado, el procesamiento continuo de documentos, los objetivos del sistema y atributo de destino del sistema. De existir un cambio debe notificarse al administrador.
- Estrategia activa, para detectar si el sistema podría colapsar al ser atacado: se utiliza una serie de secuencia de comandos de ataques que simulan el comportamiento del sistema, posteriormente se analizan los resultados; su objetivo es probar e identificar las vulnerabilidades de la red conocida. Este tipo de técnica es utilizada para ensayos de penetración y seguridad, y su uso puede afectar el rendimiento de las redes.

3.2.1. Identificación de amenazas

Para la identificación de amenazas es necesario conocer los tipos de ataques, la forma como los *hackers* pueden acceder y operar en el sistema y cuáles pueden ser los puntos que estos desean alcanzar.

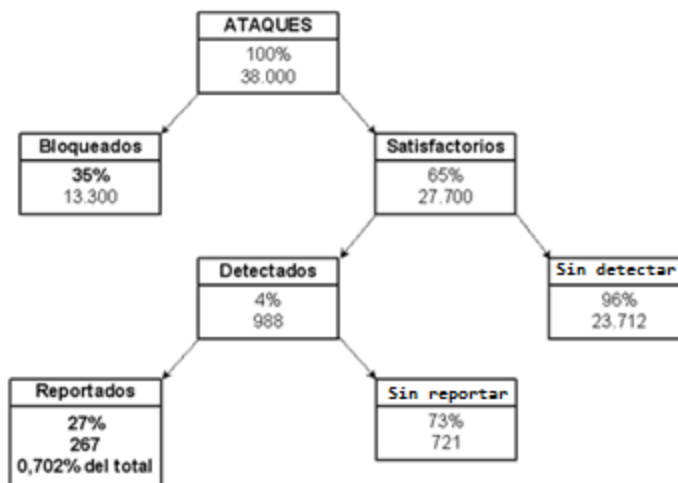
Posterior a un ataque, las consecuencias que estos ocasionan pueden clasificarse en:

- *Data Corruption*: la información que no contenía defectos pasa a tenerlos.
- *Denial of Service (DOS)*: servicios que deberían estar disponibles no lo están.
- *Leakage*: los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta la actualidad, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

El resultado de los ataques de 1992 a 1995, son presentados a continuación en la figura 3:

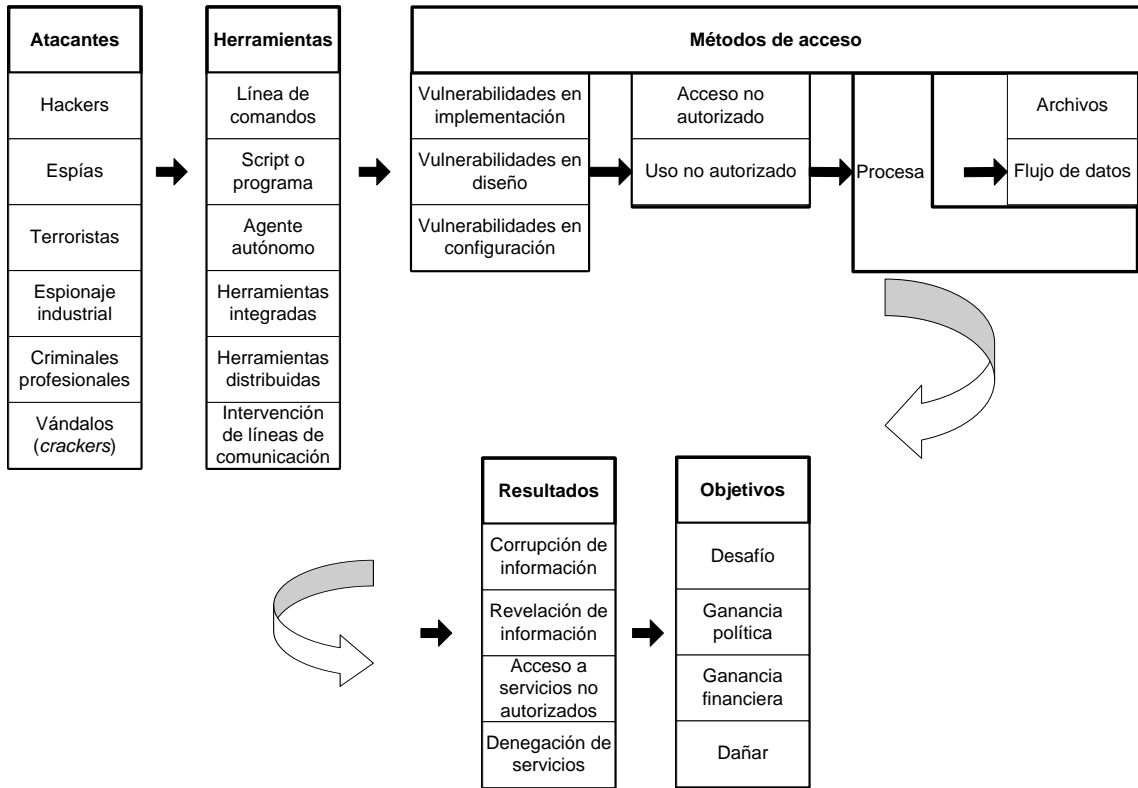
Figura 3. **Porcentaje de ataques**



Fuente: www.disa.mil. Consultado el 13 de diciembre de 2010.

La siguiente gráfica detalla el tipo de atacante, las herramientas utilizadas, en qué fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.

Figura 4. Detalle de ataques



Fuente: elaboración propia.

3.2.2. Estadísticas del CERT (Computer Emergency Response Team) – Datos históricos

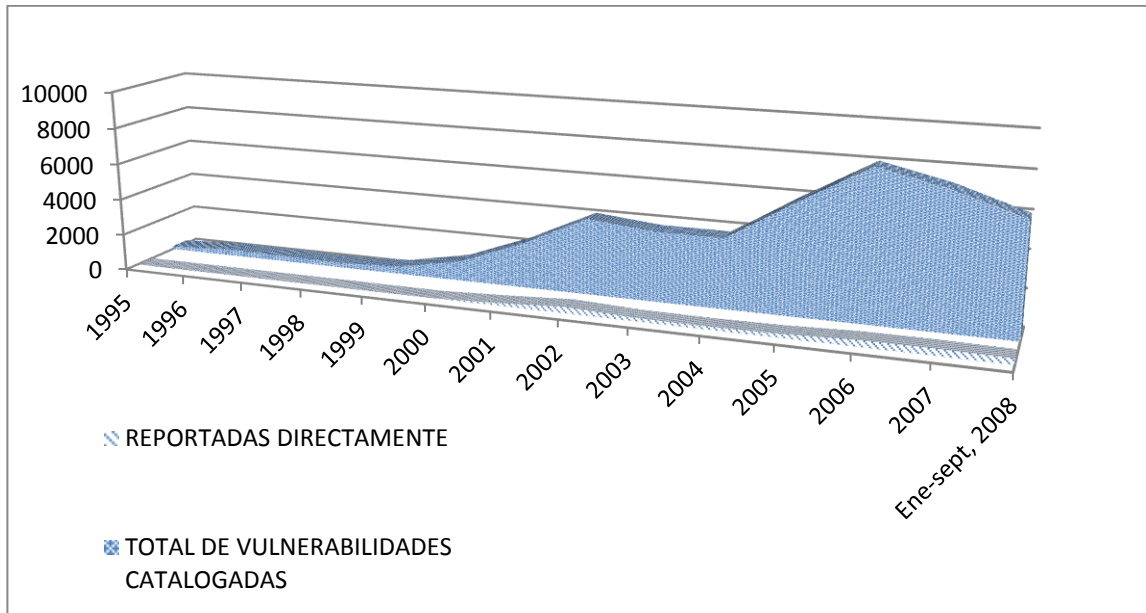
El equipo de CERT se centra en la investigación y educación para ayudar a los administradores de sistemas, desarrolladores, operadores y compradores de *software* para que sus sistemas tengan el menor número de vulnerabilidades posibles.

Tabla II. **Vulnerabilidades catalogadas por CERT**

Año	Total de vulnerabilidades catalogadas	Reportadas directamente
1995	171	
1996	345	
1997	311	
1998	262	
1999	417	
2000	1 090	
2001	2 437	153
2002	4 129	343
2003	3 784	191
2004	3 780	170
2005	5 990	213
2006	8 064	345
2007	7 236	357
Enero-septiembre 2008	6 058	310

Fuente: elaboración propia.

Figura 5. **Vulnerabilidades catalogadas**



Fuente: elaboración propia.

Definición de columnas:

Año: representa el año del calendario.

Total vulnerabilidades catalogadas: refleja el número total de vulnerabilidades que se han catalogado, basadas en informes de fuentes públicas y las presentadas directamente a CERT.

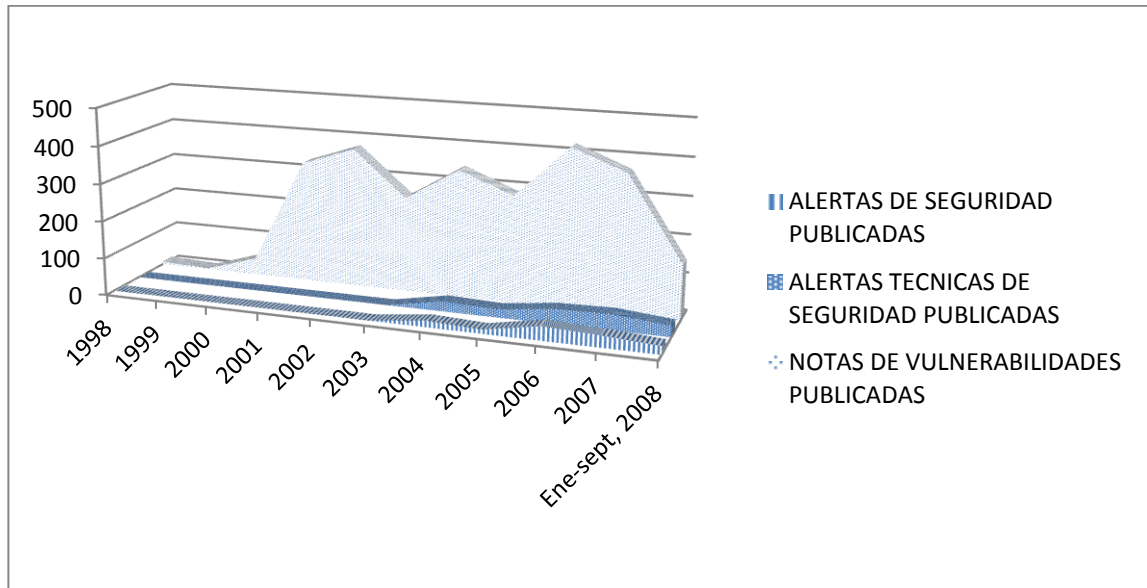
Reportadas directamente: representa el número total de vulnerabilidades que se han catalogado con base en vulnerabilidades reportadas directamente a CERT.

Tabla III. **Publicaciones sobre vulnerabilidades**

Año	Notas de vulnerabilidades publicadas	Alertas técnicas de seguridad publicadas	Alertas de seguridad publicadas
1998	8		
1999	3		
2000	47		
2001	326		
2002	375		
2003	255		
2004	341	27	17
2005	285	22	11
2006	422	39	37
2007	366	42	31
Enero-septiembre 2008	145	29	22

Fuente: elaboración propia.

Figura 6. **Cantidad de publicaciones de vulnerabilidades**



Fuente: elaboración propia.

Definición de columnas:

Año: representa el año del calendario.

Notas de vulnerabilidades publicadas: refleja el número de notas de las vulnerabilidades publicadas en CERT. Estos documentos proporcionan información técnica y soluciones a las vulnerabilidades que son analizadas.

Alertas técnicas de seguridad publicadas: se refiere al número de alertas de seguridad técnica publicadas en relación con el US-CERT.

Alertas de seguridad publicadas: Esta columna refleja el número de alertas de seguridad publicadas en relación con el US-CERT.

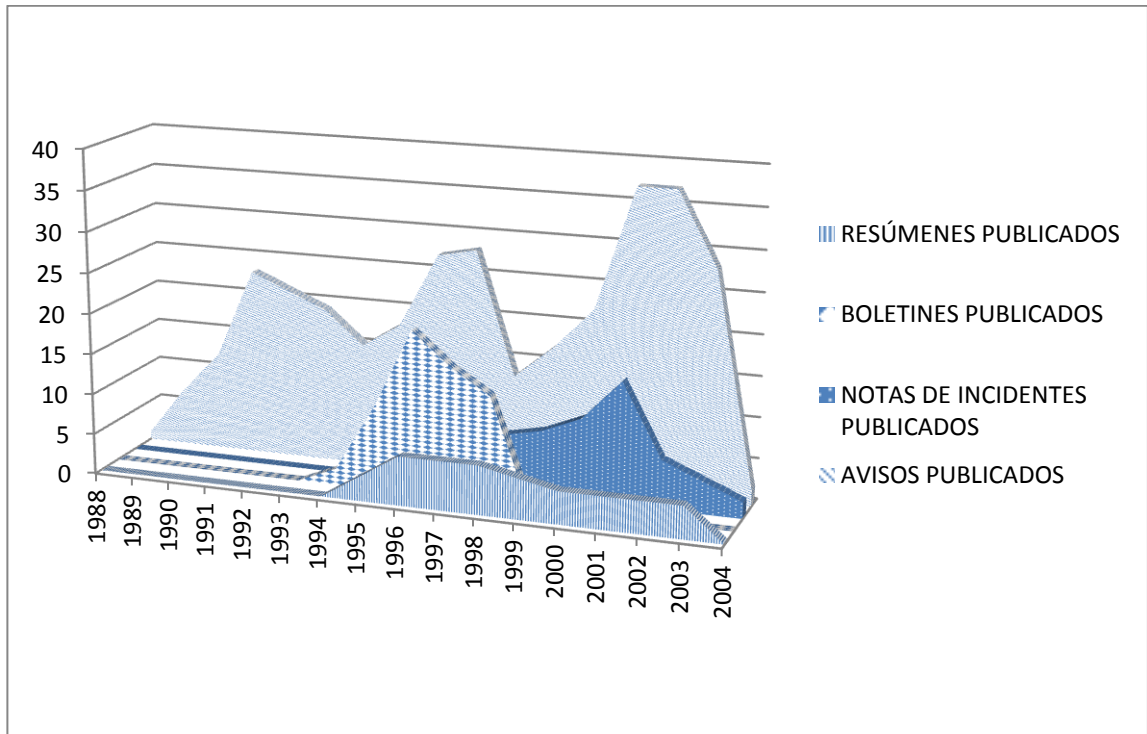
Estos documentos proporcionan información oportuna sobre cuestiones actuales de seguridad, vulnerabilidades y *exploits*.

Tabla IV. **Reporte de publicaciones 1988-2004**

Año	Avisos publicados	Notas de incidentes publicados	Boletines publicados	Resúmenes publicados
1988	1			
1989	7			
1990	12			
1991	23			
1992	21			
1993	19			
1994	15		2	
1995	18		10	3
1996	27		20	6
1997	28		16	6
1998	13	7	13	6
1999	17	8		5
2000	22	10		4
2001	37	15		4
2002	37	6		4
2003	28	4		4
2004	2	2		

Fuente: elaboración propia.

Figura 7. **Publicaciones 1988-2004**



Fuente: elaboración propia.

Definición de columnas:

Año: representa el año calendario.

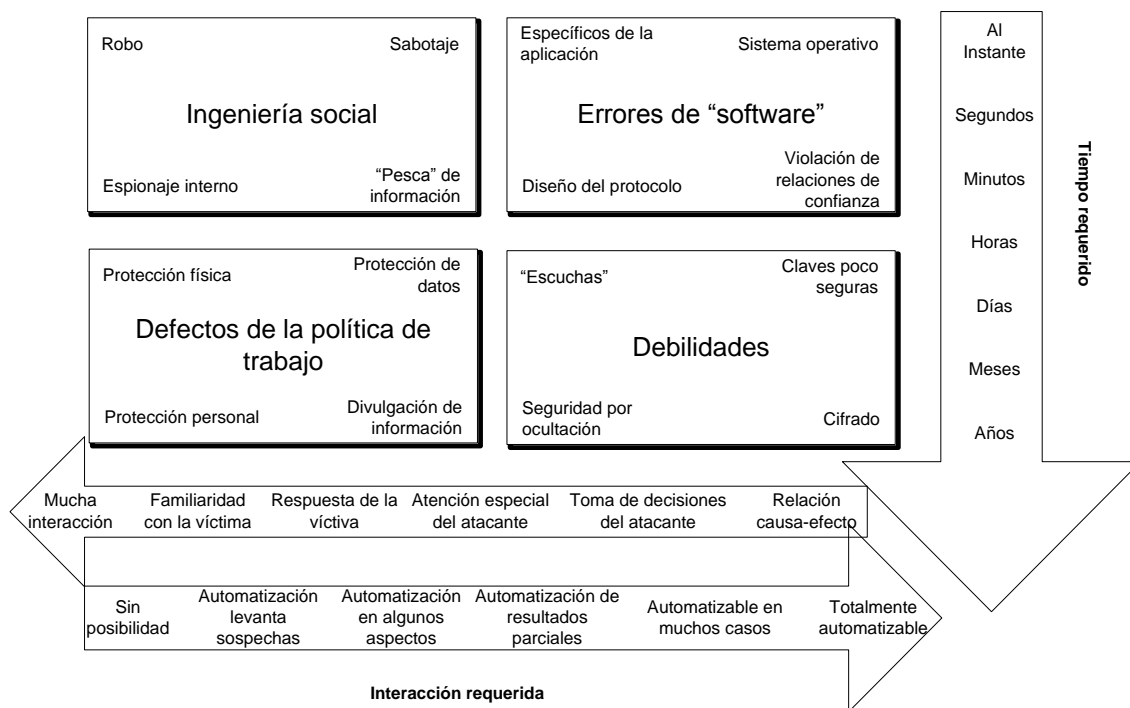
Avisos publicados: CERT proporcionó información sobre cuestiones actuales de seguridad, vulnerabilidades y exploits.

Notas de incidentes publicadas: CERT proporcionó información sobre los incidentes de la comunidad de internet.

Boletines publicados: los boletines de los proveedores tenían por objeto facilitar la distribución coordinada de información escrita por los vendedores sobre los problemas y soluciones de seguridad.

Resúmenes publicados: CERT publica cada trimestre tipos de denuncias de ataques al equipo de respuesta, así como otro incidente digno de mención y vulnerabilidad.

Figura 8. Mapa de tipo de vulnerabilidades



Fuente: http://www.ussrback.com/docs/papers/general/compvuln_draft.pdf.

Consultado el 20 de diciembre de 2010.

3.3. Herramientas para análisis

En la actualidad existe un sinfín de herramientas que brindan tanto a administradores de seguridad como a *hacker*, las vulnerabilidades que posee un sistema informático, y es deber del administrador realizar el estudio antes que su sistema sea afectado.

Previo a listar algunas de las herramientas más utilizadas para la detección de vulnerabilidades, se tiene que conocer los tipos de ataques más comunes hoy en día. A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por *hackers*. Estos pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En el inicio de los sistemas de información, los ataques involucraban poca sofisticación técnica. Los *insiders* (operadores, programadores, *data entrys*) utilizaban sus permisos para alterar archivos o registros. Los *outsiders* ingresaban a la red simplemente averiguando una contraseña válida.

Con el transcurrir de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar agujeros en el diseño, configuración y operación de los sistemas, siendo las más comunes:

- Ingeniería social
- Ingeniería social inversa
- Trashing (cartoneo)
- Ataques de monitorización
- Ataques de autenticación
- *Denial of service* (DoS)
- Ataques de modificación – daño

3.3.1. Sandcat

Es un escáner de vulnerabilidades que permite a los administradores web realizar un escaneo agresivo y comprensivo de una organización, para aislar vulnerabilidades e identificar los agujeros de la seguridad.

3.3.2. VisualRoute

Este ayuda a determinar si un problema de conectividad se debe a un ISP, Internet, o en el sitio Web de destino, e identifica la red donde se produce un problema.

3.3.3. WebInspect

Herramienta de seguridad automatizada para la evaluación de aplicaciones web y servicios de *SPI Dynamic*. Identifica vulnerabilidades conocidas y desconocidas, incluye controles que validan la configuración adecuada del servidor web. Entre las capacidades incluye el descubrimiento de todos los parámetros de entrada XML y la manipulación de parámetros en cada campo XML en busca de vulnerabilidades en el propio servicio. Requiere Windows y MSIE.

3.3.4. Nikto

Es una aplicación de código abierto (GPL); un escáner de servidor web que lleva a cabo pruebas exhaustivas de estos para varios propósitos, incluyendo más de 6400 archivos y aplicaciones potencialmente peligrosos, los controles de versiones no actualizadas de más de 1000 servidores, y los problemas de la versión específica de más de 270 servidores.

3.3.5. XProbe2

Es una herramienta de identificación de sistemas operativos (OS fingerprinting) activa, que sirve para determinar el sistema operativo de un *host* remoto.

3.3.6. Watchfire's AppScan

Suite de herramientas de Watchfire que automatiza las pruebas de seguridad de aplicaciones Web, produce análisis de defectos y ofrece recomendaciones para la fijación de las fallas de seguridad detectadas. Los módulos de evaluación pueden ser utilizados por los auditores y responsables de su cumplimiento para la realización de auditorías integrales, y validar el cumplimiento de los requisitos de seguridad.

3.3.7. Acunetix Web Vulnerability Scanner

Sitio Web para pruebas de seguridad de Acunetix; primero identifica los servidores web de una determinada IP o rango de direcciones IP, y recopila todo el sitio, reúne información sobre todos los archivos que encuentra y visualiza la estructura del sitio web. Después de esta etapa de descubrimiento, se realiza una auditoría automática para los temas de seguridad común. Aplicaciones que utilizan CGI, PHP, ASP, ASP.NET se puede comprobar en busca de vulnerabilidades como *cross site scripting*, inyección SQL, inyección de CRLF, la ejecución de código, recorrido de directorios y más. Requiere Windows y MSIE.

3.3.8. Codenomicon HTTP Test Tool

Herramienta para descubrir y erradicar fallas de seguridad en las implementaciones de HTTP a través de pruebas de robustez. Sistemáticamente genera un gran número de mensajes de protocolo que contiene elementos excepcionales simulando ataques maliciosos, con el fin de inducir accidentes componente, el ahorcamiento y las situaciones de denegación de servicio que puedan afectar al componente y la seguridad de aplicaciones. (Implementaciones de HTTP pueden ser utilizados en los servidores Web, navegadores, aplicaciones de red, servidores proxy, los analizadores de protocolo, PDAs y teléfonos celulares.)

3.3.9. SecurityMetrics Appliance

El *software* integrado y el dispositivo de *hardware* incluyen detección de intrusos y sistemas de prevención y evaluación de la vulnerabilidad. Funciona como un puente de capa 2, no se necesita configuración de la red. Descarga automáticamente las últimas firmas de ataques IDS, guiones de evaluación de la vulnerabilidad y mejoras de todas las noches.

3.3.10. Lightning Console

Herramienta de Gestión de la seguridad de *Tenable Network Security*, para la seguridad múltiple y los administradores de red a través de múltiples organizaciones. Vulnerabilidad de análisis programado, el análisis de identificadores de sucesos en tiempo real, gestión de activos, gestión de remediación de vulnerabilidades, detección de redes topología de organización y presentación de informes ejecutivos para cientos de administradores a través de interfaz web fácil de usar.

3.3.11. SARA

Security Auditor's Research Assistant herramienta de análisis de seguridad basados en Unix, Investigación Avanzada Corp. Apoya el FBI / SANS Top 20 Consenso; autoexploración a distancia y las instalaciones de la API; plug-in para la instalación de aplicaciones de terceros; SANS / ISTS certificada, actualizada cada dos meses, en apoyo a las normas CVE; basado en el modelo de SATAN. Programas de dominio público. También está disponible el *Tiger Analítica Research Assistant* (TARA), una actualización para TAMU “programa tigre” conjunto de secuencias de comandos que escanean un sistema Unix de los problemas de seguridad.

3.3.12. Qualys Free Security Scans

Seguridad gratuita de varios servicios de exploración Qualys, Inc., incluyendo *SANS / FBI Top 20 vulnerabilities Scan*, análisis de la red de seguridad, y el navegador herramienta de chequeo.

3.3.13. Qualys Guard

Servicio en línea que hace las evaluaciones a distancia de seguridad de red, gestionando la evaluación de la vulnerabilidad, dentro y fuera del *firewall*.

3.3.14. Perimeter Check

Servicio de análisis de dispositivos externos de red como servidores, sitios web, *firewalls*, *routers*, y más por las vulnerabilidades de seguridad que pueden dar lugar a interrupción del servicio, el robo de datos o sistema de destrucción. Incluye instrucciones para ayudar a solucionar los problemas de

seguridad de inmediato. Puede programar automáticamente evaluación de la vulnerabilidad de las direcciones IP, designadas en tiempos de poco tráfico.

3.3.15. STAT Scanner

Herramienta de Harris Corp. para el análisis de seguridad de Windows / UNIX / Linux y otros recursos. Utiliza bases de datos exhaustivos vulnerables, para detectar automáticamente las vulnerabilidades y debilidades.

Las capacidades incluyen: exploración y análisis de un dominio de toda la red y selección de una sola máquina, o ignorar las vulnerabilidades específicas de los archivos de configuración, los informes de análisis de vulnerabilidades con información detallada relacionada con el nombre de descripción y nivel de riesgo de cada punto vulnerable; para eliminar las vulnerabilidades, se recomienda el uso *retest* soluciones con enlaces a sitios web relacionados.

3.3.16. Nessus Security Scanner

Herramienta de código abierto de seguridad a distancia para auditoría de red, creada por Renaud Deraison, se basa en: "nunca confíes en el número de versión" y "nunca confíes en que un determinado servicio está escuchando en el puerto bueno". Nessus se compone de dos partes: un servidor y un cliente, el servidor (nessus) gestiona los "ataques", mientras que el cliente es un interfaz diseñado para recoger los resultados. Incluye más de 1000 pruebas en 23 categorías de vulnerabilidad, y Nessus Attack Scripting Language. Funciona con una variedad de sistemas operativos.

3.3.17. Secure-Me

Prueba automática de análisis de seguridad de servicios de Broadbandreports.com para máquinas individuales, puertos escaneos, servicios de revisión denegados, 45 servidores comunes en comprobaciones de vulnerabilidad del servidor, servidor web de referencia, peticiones por segundo, y una amplia variedad de otras pruebas. Versiones limitadas con licencia libre o completo disponible.

3.3.18. SAIN

Security Administrator's Integrated Network herramienta de pruebas de seguridad de SAINT Corporation. Una versión actualizada y mejorada versión de la herramienta de red SATAN pruebas de seguridad, actualizadas regularmente, CVE compatibles. Incluye pruebas de denegación de servicio, informes que especifican los niveles de gravedad de los problemas, de un único aparato o barridos completos de la red.

También se dispone de autoguiados WebSAINT servicio de barrido, y el aparato SAINTbox escáner. Funciona con muchos sabores de Unix.

3.3.19. NMap Network Mapper

Utilidad libre de código abierto para la exploración de red o de auditoría de seguridad, diseñado para explorar rápidamente grandes redes o *hosts* individuales. Usos o paquetes IP en nuevas formas para determinar qué *hosts* están disponibles en la red, qué servicios (puertos) están ofreciendo, qué sistema operativo (y versión de sistema operativo) se está ejecutando, qué tipo

de filtros o *firewall* se está utilizando, y muchas otras características. Funciona en la mayoría de las versiones de UNIX, así como Windows.

3.3.20. NetIQ Security Analyzer

Multiplataforma de escaneo de compatibilidad y evaluación del producto. Los sistemas son analizados a la vista o en intervalos programados; servicio de actualización automática que permite una actualización con las pruebas de seguridad más recientes. Incluye un kit del desarrollador de *software* personalizado para permitir adiciones test de seguridad, para Windows / Solaris / Linux

3.3.21. Foundstone

Software de administración de vulnerabilidad de *McAfee / Network Associates* puede proporcionar evaluaciones de la vulnerabilidad global de la empresa, la remediación de información, etc. Disponible como dispositivo *hardware*, o de servicios gestionados.

3.3.22. CERIAS Security Archive

La Universidad de Purdue Centro de Educación e Investigación en Aseguramiento de la Información y el sitio de Seguridad, incluye amplia colección de enlaces, organizados por temas, a los centenares de recursos de información y herramientas de seguridad, los recursos de detección de intrusos, la ley de electrónicos, publicaciones, etc. También incluye un sitio FTP con una gran colección de los servicios públicos relacionados con la seguridad, escáneres, herramientas de detección de intrusos, etc.

3.3.23. Internet Scanner

Herramienta de Internet Security Systems, provee evaluación de la vulnerabilidad, medición automática de riesgos de seguridad en línea. Realiza regulares escaneos para la selección de los servicios de red, servidores, ordenadores de sobremesa, sistemas operativos, *routers*, *firewalls*, etc. para descubrir e informar las vulnerabilidades de los sistemas que pueden estar abiertos a los ataques.

Proporciona informes flexibles de gestión de riesgos y asesoramiento, prepara arreglos, análisis de tendencias y datos completos conjuntos para apoyar la aplicación de políticas y servicios similares gestionados también disponibles.

3.4. Análisis interno

Cuando se estudia un sistema para implementar un sistema de seguridad, este no tiene que estar destinado a proteger el sistema solo contra ataques provenientes del exterior, también debe brindar la protección desde adentro de la organización.

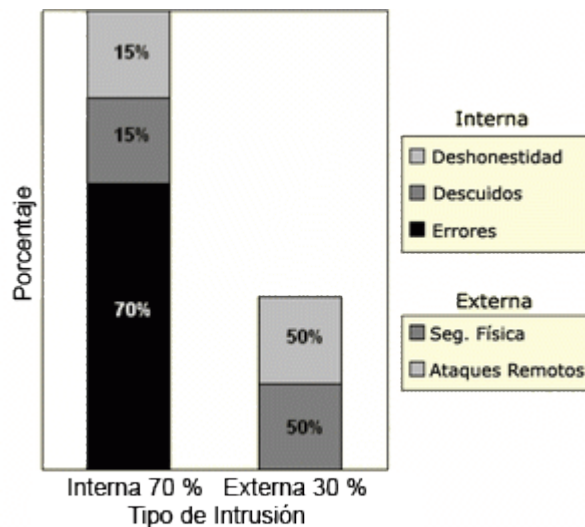
Dentro de una organización cualquier usuario puede ser una amenaza potencial, si no se tiene el adiestramiento necesario para manejar de forma correcta sus roles y responsabilidades.

3.4.1. Personal – insiders

La mayoría de las ocasiones a los usuarios se les muestra como víctimas de agentes externos, pero estudios recientes sobre robos, sabotajes o accidentes que tienen relación con los sistemas informáticos, muestran que el 70% es causado por personal interno de la organización propietaria de dichos sistemas.

En el siguiente gráfico se detallan los porcentajes de intrusiones, clasificando a los atacantes en internos y externos.

Figura 9. **Porcentaje de intrusiones**



Fuente: <http://www.cybsec.com>. Consultada el 10 de diciembre de 2010.

Estas cifras pueden ser preocupantes, debido a que, cualquier persona que labore dentro de la organización, que conozca el sistema a la perfección, tanto sus puntos fuertes como débiles, podría realizar un ataque más directo, difícil de detectar y más efectivo, en comparación con cualquier ataque proveniente del exterior.

Existen gran variedad de motivos que pueden llevar a una persona a cometer cualquier tipo de delito informático contra su propia organización, pero sin importar los motivos, estos deben prevenirse y evitarse.

Como ya se ha mencionado, los ataques pueden ser del tipo pasivo o activo, y el personal realiza ambos indistintamente dependiendo de la situación concreta.

El tipo de ataques que podemos encontrar en zonas internas de la organización pueden venir de:

- Personal interno
- Ex-empleado
- Curiosos
- Terroristas
- Intrusos remunerados
- Recomendaciones

En la actualidad, con el crecimiento que han tenido los dispositivos inalámbricos, la mayoría de organizaciones han optado por utilizar estas tecnologías, sin embargo, en ocasiones suelen pasar por alto aspectos de seguridad, logrando que el acceso a una red sea tan fácil como tener un dispositivo que posea conexión inalámbrica.

También se tiene otra vulnerabilidad: existen puntos de red que cualquier persona que tenga acceso a la ubicación de esta, podría conectarse fácilmente.

Como ejemplo de estos dos aspectos que abarcan una vulnerabilidad específica, está el acceso a la red de la Facultad de Ingeniería, que si bien es una red pública, en organizaciones se ven los mismos casos, como tener su red inalámbrica sin protección y los puntos de red descubiertos. Un ejemplo gráfico se observa en la figura 10.

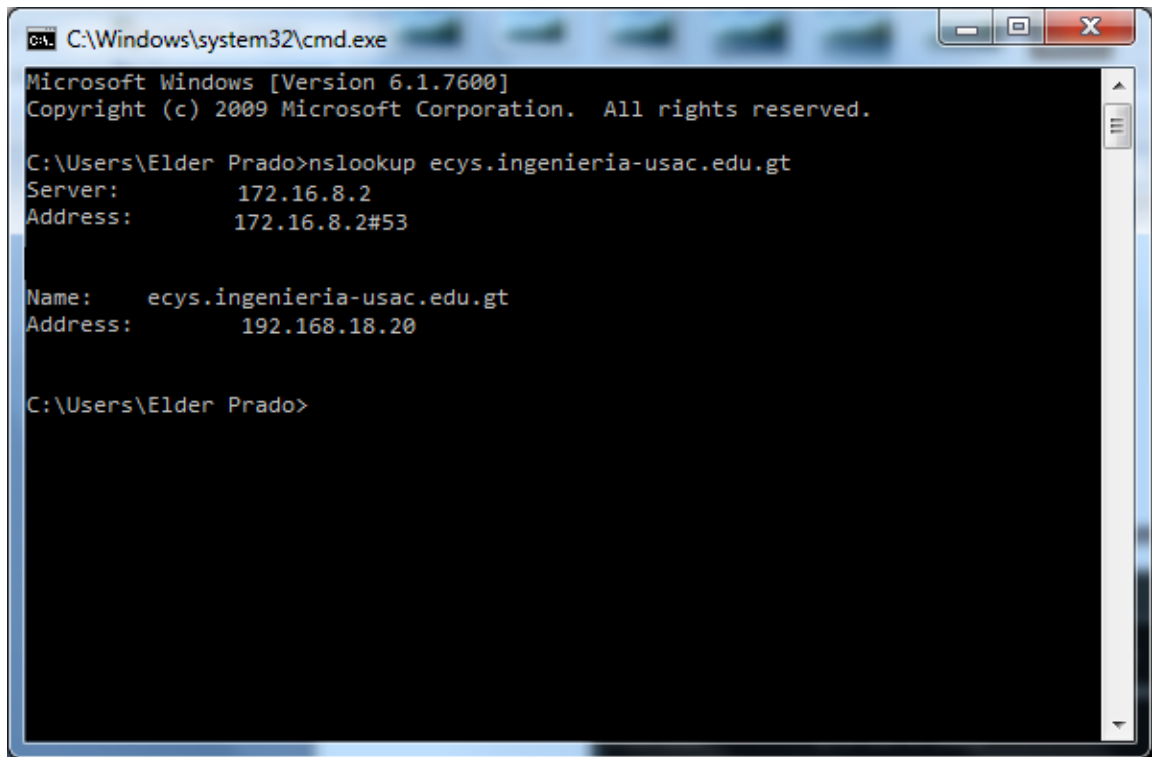
Figura 10. **Punto de red vulnerable**



Fuente: Fotografía tomada en edificio T-3 Facultad de Ingeniería, USAC.

Una vez dentro de la red de las organizaciones existen herramientas que pueden proveer al atacante información acerca de los equipos y servidores, si estos no se encuentran aislados dentro de una DMZ. Si se conoce información de que los servidores se encuentran dentro de la misma red, la dirección IP puede ser ubicada fácilmente por medio del comando nslookup, aunque la respuesta por medio del protocolo ICMP esté desactivada.

Figura 11. **Uso del comando nslookup**



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Elder Prado>nslookup ecys.ingenieria-usac.edu.gt
Server:         172.16.8.2
Address:        172.16.8.2#53

Name:   ecys.ingenieria-usac.edu.gt
Address: 192.168.18.20

C:\Users\Elder Prado>
```

Fuente: Ejecución de comando nslookup, en red pública de Facultad de Ingeniería, USAC.

Con el comando nmap se puede obtener información acerca de alguno de los servidores, como sistema operativo listado de puertos abiertos.

Los resultados obtenidos son los siguientes:

Interesting ports on srvvac.ccie.edu (172.16.8.2):

Not shown: 970 closed ports

PORT STATE SERVICE

7/tcp open echo

9/tcp open discard

13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
22/tcp open ssh
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1026/tcp open LSA-or-nterm
1029/tcp open ms-lsa
1059/tcp open nimreg
1066/tcp open fpo-fns
1071/tcp open unknown
1079/tcp open unknown
1723/tcp open pptp
2161/tcp open apc-agent
2222/tcp open unknown
3052/tcp open powerchute
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
8000/tcp open http-alt
8085/tcp open unknown
8086/tcp open unknown
MAC Address: 00:02:A5:EA:65:50 (Hewlett Packard)

No exact OS matches for host (If you know what OS is running on it, see <http://nmap.org/submit/>).

También se encuentra información del *firewall* que se encuentra en la red:

Interesting ports on map1.ingenieria-usac.edu.gt (192.168.18.1):

Not shown: 999 filtered ports

PORT STATE SERVICE

21/tcp open ftp

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING) : OpenBSD 4.X (85%)

Aggressive OS guesses: OpenBSD 4.3 (85%), OpenBSD 4.0 (85%)

No exact OS matches for host (test conditions non-ideal).

Y cuenta con un puerto abierto dado que es el FTP; puede darse el caso de tener habilitado el acceso por medio de cuenta anónima; también otra falla es que se tiene información sobre el sistema operativo, y con un poco de investigación, es probable encontrar las vulnerabilidades para este sistema.

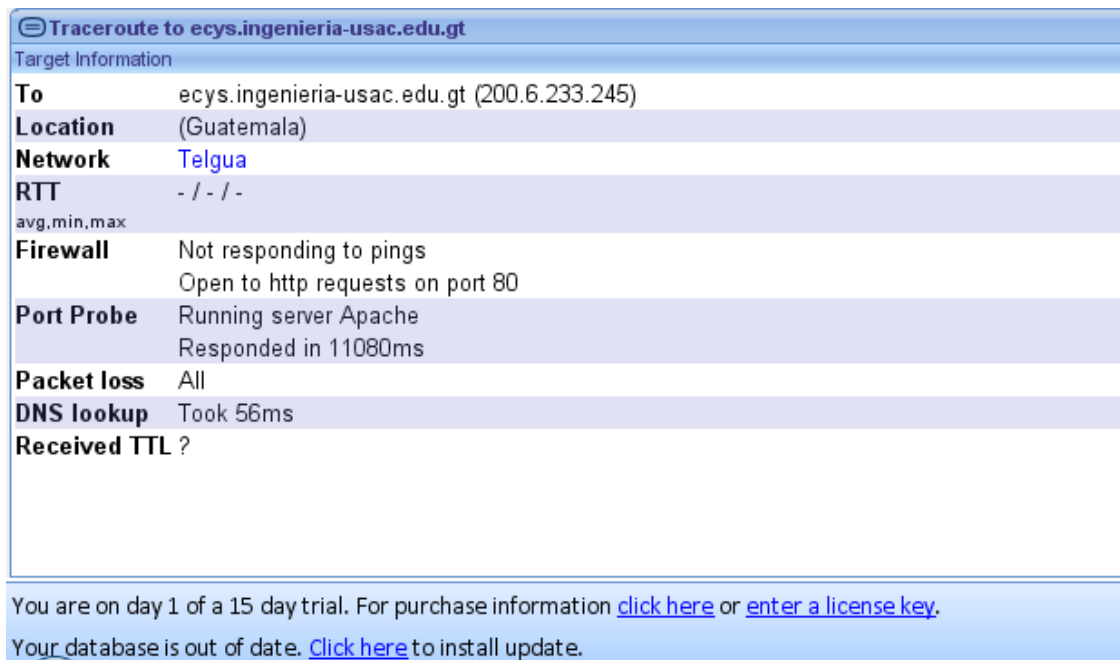
3.5. Análisis externo

Al referirse a realizar el análisis externo de vulnerabilidades, vale la pena mencionar que es casi imposible que cualquier amenaza externa afecte al sistema de forma accidental; siempre este ataque será de alguna persona que busca explotar dicha vulnerabilidad.

Para la realización de un ataque o explotar alguna vulnerabilidad, las personas que realizan este tipo de acciones, poseen un alto nivel de conocimiento sobre redes, sistemas operativos y sobre la organización.

Con el uso de las herramientas se puede indagar ciertas cosas de la organización, que en la mayoría de casos, se piensa que nadie puede conocer esta información. La herramienta VisualRoute2010 brinda cierta información sobre la red que puede ser utilizada por los *hackers*, para explotar vulnerabilidades y realizar ataques:

Figura 12. Información obtenida con Aplicación Visual Route 2010



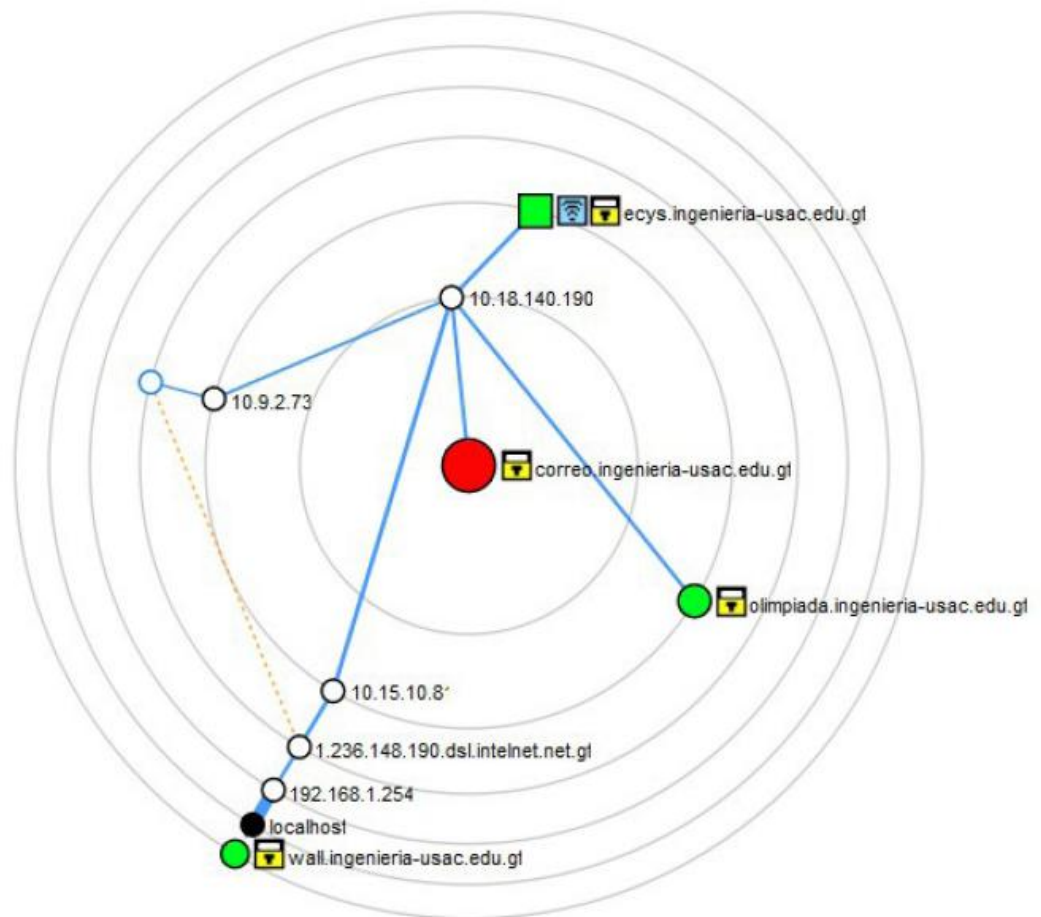
Target Information	
To	ecys.ingenieria-usac.edu.gt (200.6.233.245)
Location	(Guatemala)
Network	Telgua
RTT	- / - / - avg, min, max
Firewall	Not responding to pings Open to http requests on port 80
Port Probe	Running server Apache Responded in 11080ms
Packet loss	All
DNS lookup	Took 56ms
Received TTL ?	

You are on day 1 of a 15 day trial. For purchase information [click here](#) or [enter a license key](#).
Your database is out of date. [Click here](#) to install update.

Fuente: elaboración propia.

También se puede obtener información acerca de los dispositivos que se encuentran en la red:

Figura 13. **Gráfico obtenido con Visual Route 2010**



Fuente: elaboración propia.

Con la herramienta xProbe2 se puede obtener información del servidor que se esté analizando:

Nombre del dispositivo: ecys.ingenieria-usac.edu.gt

Dirección IP privada: 172.16.8.2

Dirección IP pública: 200.6.233.245

Análisis de puertos:

Tabla V. **Tabla de análisis de puertos**

Puerto	Estado	Servicio	Versión
TCP 80	Abierto	http	Apache httpd
TCP 443	Abierto	https	Apache httpd sslv2
TCP 222	Abierto	ssh	Protocol 2.0
TCP 21	Abierto	ftp	Microsoft ftpd
TCP 25	Abierto	smtp	
TCP 135	Abierto	msrpc	Microsoft Windows msrpc
TCP 5800	Abierto	vnc-http	RealVNC 4.0
TCP 5900	Abierto	vnc	VNC 3.8

Fuente: elaboración propia.

3.5.1. Vulnerabilidades identificadas

Luego de realizado un análisis sobre el sistema, utilizando algunas de las herramientas expuestas anteriormente, se lograron detectar algunas vulnerabilidades las cuales se describen a continuación:

3.5.1.1. Módulo de PHP My_eGallery (NIKTO)

Exploits encontrados:

- MDPPro Module My_eGallery (pid) Remote SQL Injection Exploit
- XOOPS Module My_eGallery 3.04 (gid) SQL Injection Vulnerability
- PHP-Nuke My_eGallery <= 2.7.9 Remote SQL Injection Vulnerability
- myphpNuke Module My_eGallery 2.5.6 (basepath) RFI Vulnerability

3.5.1.2. Método HTTP TRACE (NIKTO)

Esta activo, se supone que es vulnerable vía para XST.

3.5.1.3. Servicio RealVNC versión 4.0 (NMAP)

Búsqueda de *exploits* en exploit-db.com los resultados fueron que no existen *exploits* para esta versión, pero sí para las versiones 4.1.0.

3.5.1.4. Servidor Web Microsoft IIS 6.0 (NMAP)

Exploits encontrados:

- Microsoft IIS 6.0 WebDAV Remote Authentication Bypass Exploit (pl)
- Microsoft IIS 6.0 WebDAV Remote Authentication Bypass Exploit (php)
- Microsoft IIS 6.0 WebDAV Remote Authentication Bypass Exploit (patch)
- Microsoft IIS 6.0 WebDAV Remote Authentication Bypass Vulnerability

3.5.1.5. Plataforma Dokeos 1.8.5

Exploits encontrados:

- Dokeos LMS <= 1.8.5 (include) Remote Code Execution Exploit
- Dokeos LMS <= 1.8.5 (whoisonline.php) PHP Code Injection Exploit

3.5.1.6. Joomla 1.5

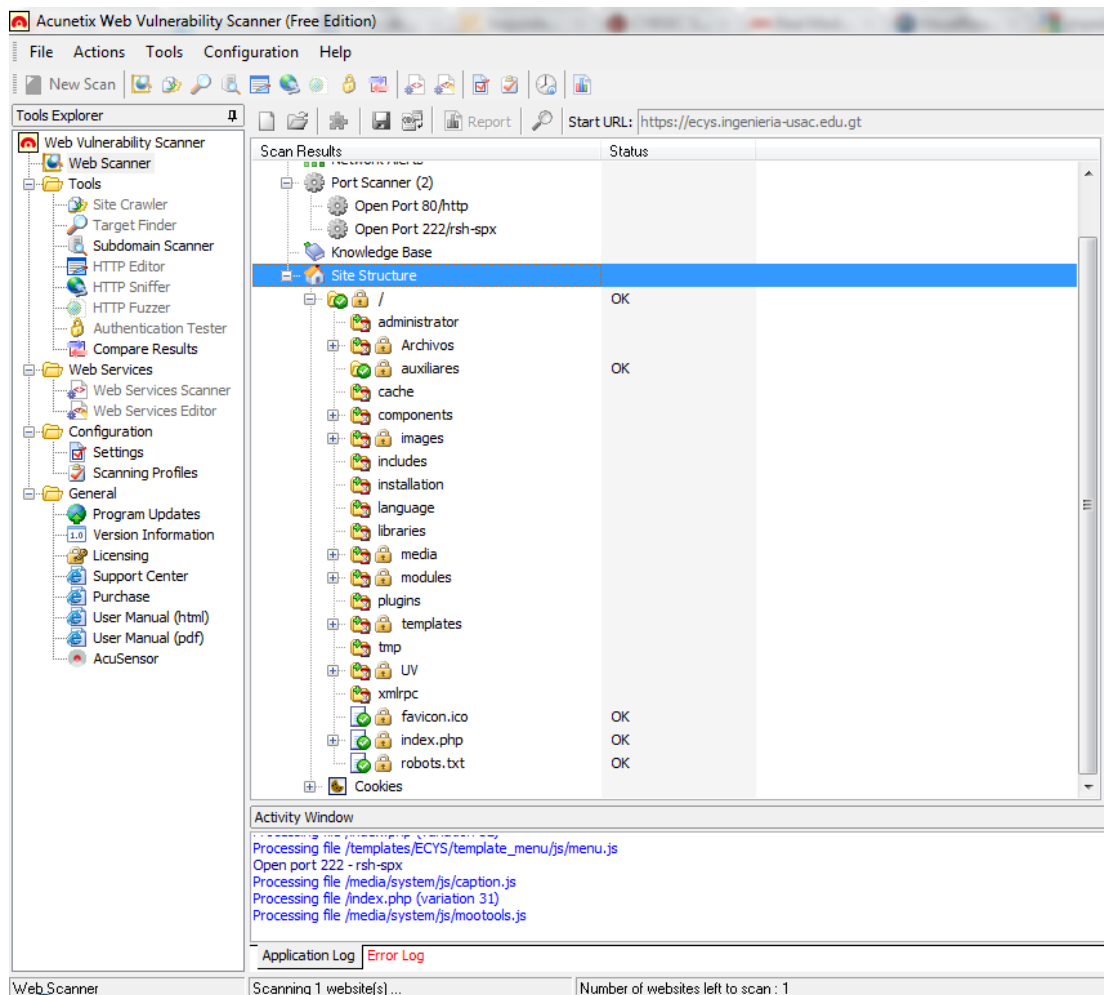
Exploits encontrados:

- Joomla 1.5 URL Redirecting Vulnerability
- Joomla 1.5 Jreservation Component SQLi And XSS Vulnerability
- Joomla 1.5.x com_joomgallery&func Incorrect Flood Filter
- Joomla 1.5.0 Beta (pcltar.php) Remote File Inclusion Vulnerability
- Joomla <= 1.5.8 (xstandard editor) Local Directory Traversal Vulnerability

Con la aplicación *Acunetix Web Vulnerability Scanner*, se obtienen entre otros aspectos, las estructuras del servidor web, y si no se cuenta con las

restricciones necesarias, cualquier persona podría acceder a contenidos confidenciales.

Figura 14. Pantalla de la herramienta Acunetix



Fuente: elaboración propia.

También se debe hacer la aclaración que aunque hablando de tecnologías, el servidor cuente con la seguridad necesaria, también debe enfocarse en el nivel de aplicaciones, ya que la mayoría de veces se gasta mucho en infraestructura y se descuida la parte de las aplicaciones.

Siguiendo con el ejemplo estudiado, lo que es común encontrar en la mayoría de sitios, es que a pesar de utilizar el lenguaje php en sus páginas, aún se ven accesos por medio de métodos GET, y solo con esto se crea una vulnerabilidad, que personas puedan acceder a recursos que no deberían de visualizar, rompiendo con el principio de menor privilegio.

Figura 15. **Vulnerabilidad por medio del método GET**



Fuente: Página de Escuela de Ciencias y Sistemas, Facultad de Ingeniería USAC.

Otra de las vulnerabilidades más comunes encontradas, es la denegación de servicios (DoS), que su solución se proporcionará en el siguiente capítulo.

4. REDUCCIÓN DE RIESGOS – APLICACIÓN DE POLÍTICAS DE SEGURIDAD

4.1. Reducción de riesgos

La reducción de riesgos implica priorizar, evaluar y aplicar las correspondientes fases de los controles recomendados por el proceso de evaluación de riesgos.

Debido a que la eliminación de todos los riesgos es por lo general poco práctica o casi imposible, es responsabilidad de los altos directivos y gerentes, utilizar el enfoque basado en reducción de costos y aplicar los controles más adecuados para disminuir el riesgo a un nivel aceptable.

4.1.1. Opciones en la reducción de riesgos

La reducción de riesgos es una metodología sistemática que es utilizada por la alta gerencia para reducir o prevenir los riesgos a los que se encuentran expuestas las organizaciones.

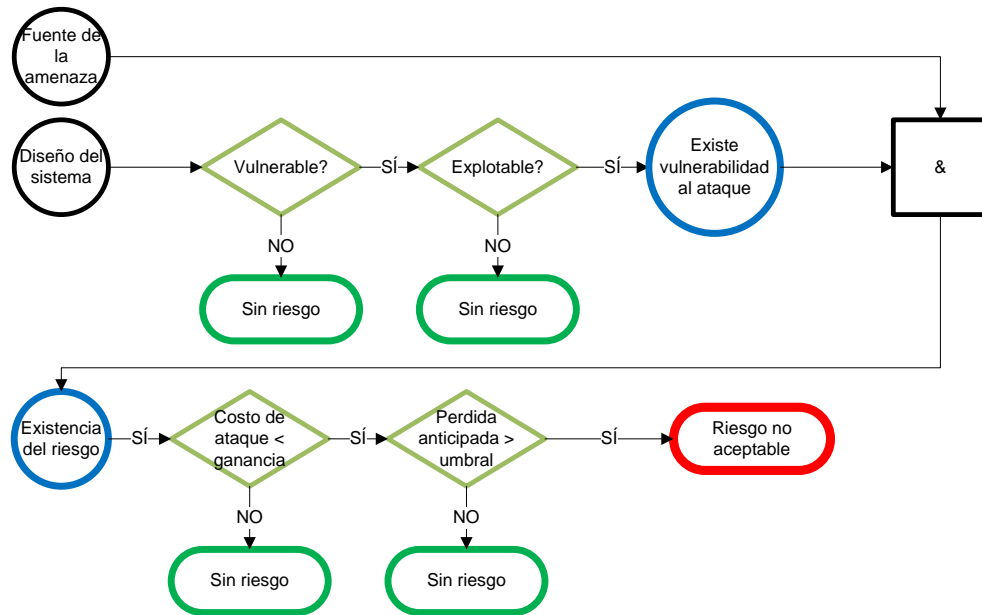
Para lograr la reducción de riesgos se toma cualquiera de las siguientes opciones:

- Asumir el riesgo: se acepta el riesgo potencial y el sistema de TI continúa operando; otra opción es implementar controles para los riesgos menores y así tener un nivel aceptable de riesgo.

- Prevención de riesgos: para evitar el riesgo, se eliminan todas aquellas causas que conllevan a la generación del mismo.
- Limitación del riesgo: las consecuencias del riesgo se pueden limitar, mediante la implementación de controles que reduzcan al mínimo los efectos adversos de una amenaza ante una vulnerabilidad.
- Planificación de riesgo: el riesgo se administra mediante un plan que consiste en la aplicación y mantenimiento de los controles.
- Investigación y reconocimiento: para reducir el riesgo de pérdida por no reconocer la vulnerabilidad o falla, se investiga el uso de controles para corregir la vulnerabilidad.
- La transferencia de riesgos: el riesgo es transferido hacia otras personas o departamentos que puedan respaldar al sistema.

Entre los objetivos principales de las organizaciones debe considerarse cualquier forma de reducir los riesgos, aunque la mayoría de las ocasiones no puede atacarse todos, se debe establecer prioridad respecto del daño que puedan causar a la organización.

Figura 16. Estrategia de reducción de riesgos

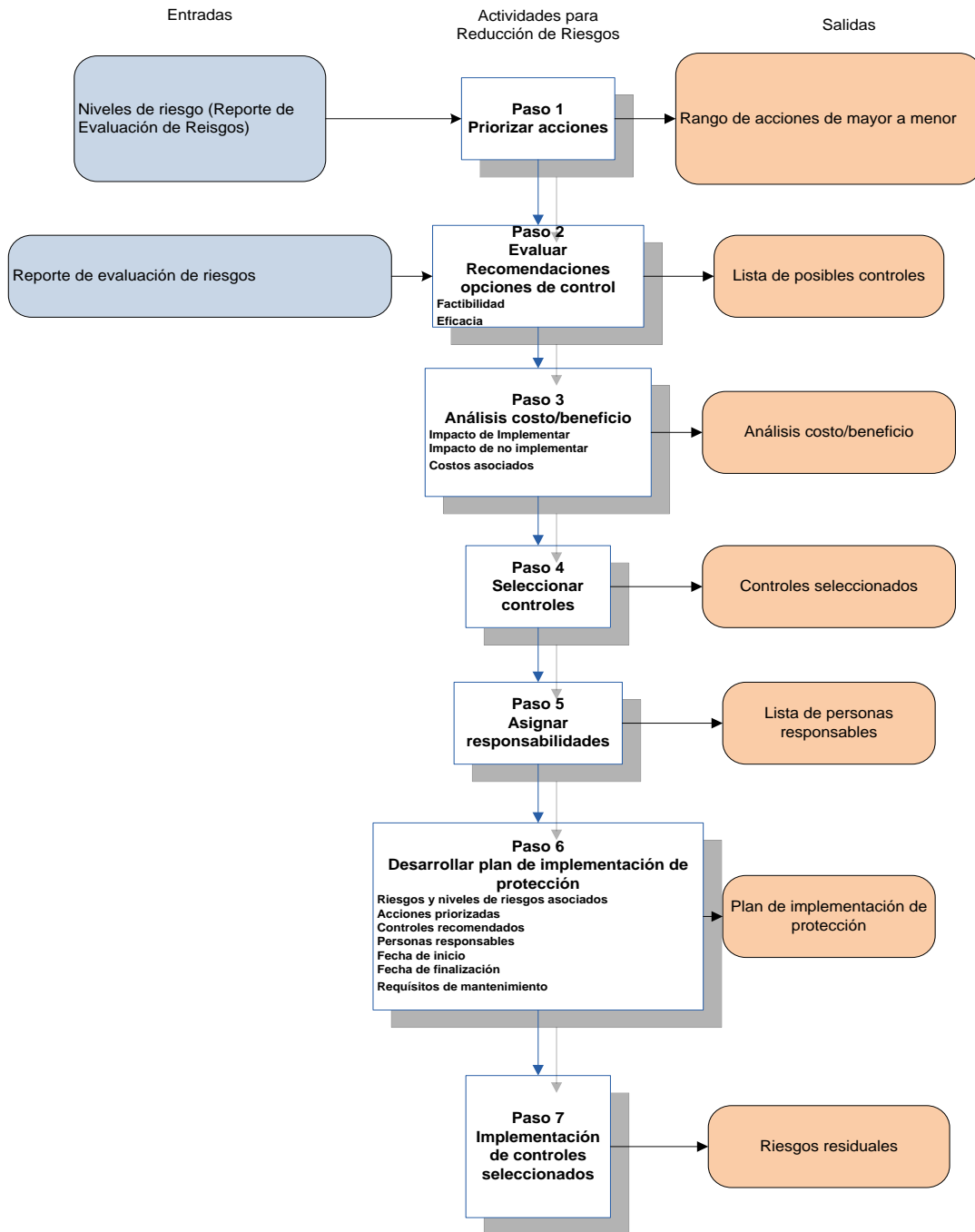


Fuente: elaboración propia

Esta estrategia que se muestra en la figura 16, se basa en reglas fundamentales, las cuales proporcionan una guía sobre forma de medición para reducir los riesgos de las amenazas humanas intencionales:

- Existencia de la vulnerabilidad: cuando se conoce sobre la existencia de alguna vulnerabilidad, se deben aplicar técnicas que garanticen la reducción de que puedan perjudicarnos por medio de esta.
- Explotar una vulnerabilidad: cuando a pesar de todo no se logra eliminar la vulnerabilidad y esta puede ser explotada con fines dañinos, se busca la creación de controles que permitan reducir al máximo las amenazas potenciales y el impacto que estas puedan causar.

Figura 17. Propuesta para implementación de controles



Fuente: elaboración propia.

4.1.1.1. Priorizar acciones

Con base en los niveles de riesgo presentados en el informe de evaluación de riesgos, se priorizan las medidas de aplicación. En la asignación de recursos, la máxima prioridad debe darse a los elementos que en la clasificación de riesgos están marcados como inaceptables.

4.1.1.2. Evaluar recomendaciones y opciones de control

Se recomiendan los controles durante el proceso de evaluación de riesgos, estos no deben ser las opciones más simples o factibles. Durante este proceso, la factibilidad y eficacia de las recomendaciones y opciones de control son analizados. El objetivo es seleccionar la opción de control más adecuada con el objetivo de minimizar el riesgo.

4.1.1.3. Realizar análisis costo/beneficio

Para dar apoyo en la administración de toma de decisiones y para identificar los controles que son rentables, se debe realizar un análisis de costo/beneficio.

4.1.1.4. Seleccionar controles

Basado en los resultados del análisis de costo-beneficio, se determina el control de gestión más rentable para reducir el riesgo dentro de la organización. Los controles seleccionados deben combinar técnicas, operaciones, y los elementos de control de gestión, para garantizar la seguridad adecuada dentro del sistema de TI y la organización.

4.1.1.5. Asignar responsabilidades

Se identifican personas adecuadas que tienen los conocimientos y habilidades adecuadas para aplicar el control seleccionado, y se les asigna alguna responsabilidad.

4.1.1.6. Desarrollar plan de implementación de protección

En este paso se desarrollará un plan, que debe contener como mínimo:

- Riesgos y niveles asociados de riesgo
- Controles recomendados
- Acciones prioritarias
- Selección de los controles previstos
- Recursos necesarios para la implementación de controles previstos
- Lista de responsabilidades de equipos y personas
- Fecha de inicio de la implementación
- Fecha de conclusión
- Requerimientos de mantenimiento

4.1.1.7. Implementación de controles seleccionados

Dependiendo de las situaciones que puedan darse, independientemente de la organización, los controles implementados llegarán a reducir el riesgo, pero nunca lo eliminarán por completo.

4.2. Políticas de seguridad

En la actualidad es imposible hablar de un sistema cien por ciento seguro, y la respuesta a esto es sencilla: debido a que el costo de la seguridad total es muy elevado, muchas organizaciones aprenden a vivir con los riesgos.

En la mayoría de los casos las empresas se ven forzadas a únicamente protegerse ante determinado conjunto de vulnerabilidades. En los últimos años se han desarrollado documentos, directrices y recomendaciones que muestran el uso correcto de las nuevas tecnologías.

Las políticas de seguridad son un conjunto de herramientas, que consisten en hacer conciencia en todos los individuos que conforman las organizaciones respecto de la importancia sobre la información sensible y servicios críticos; estas permiten que las compañías se desarrollen y mantengan en ambientes de riesgos reducidos.

Una Política de Seguridad “es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema”.¹

La RFC 1244 define Política de Seguridad como: “una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán”.²

¹ HUERTA, Antonio Villalón. *Seguridad en Unix y redes*. p.259.

² REYNOLS, Joyce K.; HOLBROOK J. PAUL. *RFC 1244: Site Security Handbook*. p.23.

Las políticas de seguridad pueden verse como una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; “una política de seguridad es una forma de comunicarse con los usuarios y gerentes. Estas establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas”.³

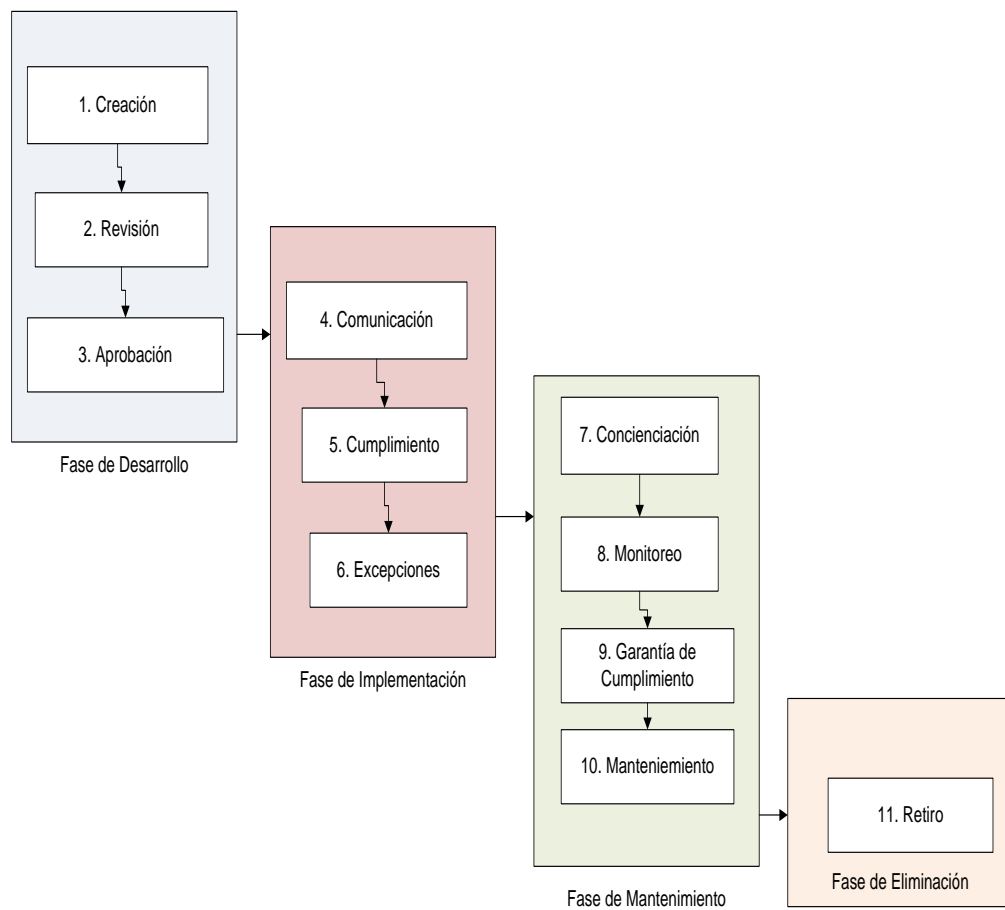
Las políticas de seguridad siempre deben de tratar de mantener los atributos de seguridad tratados en el primer capítulo de este trabajo, además, se debe aclarar que estas, no son mecanismos, ni legislaciones; si no, es una concientización de lo que se desea proteger y la razón por la cual se intenta proteger.

³ SPAFFORD, Gene. *Manual de seguridad en redes*. ArCERT. Argentina. 2000. p.17.

4.2.1. Etapas en el desarrollo de una política de seguridad

En la elaboración de políticas de seguridad, existen varias etapas por las que esta debe pasar, y están agrupadas por las siguientes fases:

Figura 18. Etapas en el desarrollo de una política de seguridad



Fuente: elaboración propia.

4.2.1.1. Fase de desarrollo

Durante esta fase, se crea la política, se revisa y se aprueba. Sus etapas son:

- **Creación:** durante esta etapa se debe identificar la necesidad que va a cubrir la política, especificar su alcance y verificar si es aplicable a la organización; también se deben nombrar a los posibles responsables y garantizar su implementación.
- **Revisión:** cuando la documentación ha sido creada, esta debe ser revisada por un grupo o individuo independiente antes de su aprobación final.
- **Aprobación:** durante esta etapa se busca obtener el apoyo para poder aplicar la política, esta etapa permite iniciar la fase de implementación.

4.2.1.2. Fase de implementación

Durante esta fase se da a conocer la política, se implementa y acata. Sus etapas son:

- **Comunicación:** durante esta etapa debe informarse a todos los individuos involucrados sobre el contenido de la política, así como las repercusiones que esta tendrá.
- **Cumplimiento:** esta etapa involucra la ejecución de la política, también incluye el adiestramiento del personal para obtener los resultados esperados.

- Excepciones: son aquellos casos especiales, en los cuales la política no puede aplicarse completamente como estaba definida al inicio.

4.2.1.3. Fase de mantenimiento

Durante esta fase se debe velar por el cumplimiento de la política por medio de un constante monitoreo, además de involucrar las políticas deben actualizarse a las necesidades actuales. Sus etapas son:

- Concienciación: durante esta etapa se busca garantizar que las personas involucradas estén conscientes de la política y busca facilitar su cumplimiento.
- Monitoreo: se busca seguir y reportar la efectividad de los esfuerzos realizados para cumplir con la política.
- Garantía de cumplimiento: esta etapa abarca las respuestas provenientes de la alta gerencia hacia los actos que vayan en contra de las políticas implementadas, para evitar que sigan siendo violadas.
- Mantenimiento: esta etapa tiene como objetivo garantizar la vigencia de la política, manteniéndola actualizada antes las necesidades actuales.

4.2.1.4. Fase de eliminación

Algunas políticas tienen validez sólo por cierto tiempo o determinada actividad, esta fase se refiere al momento en que la política será retirada.

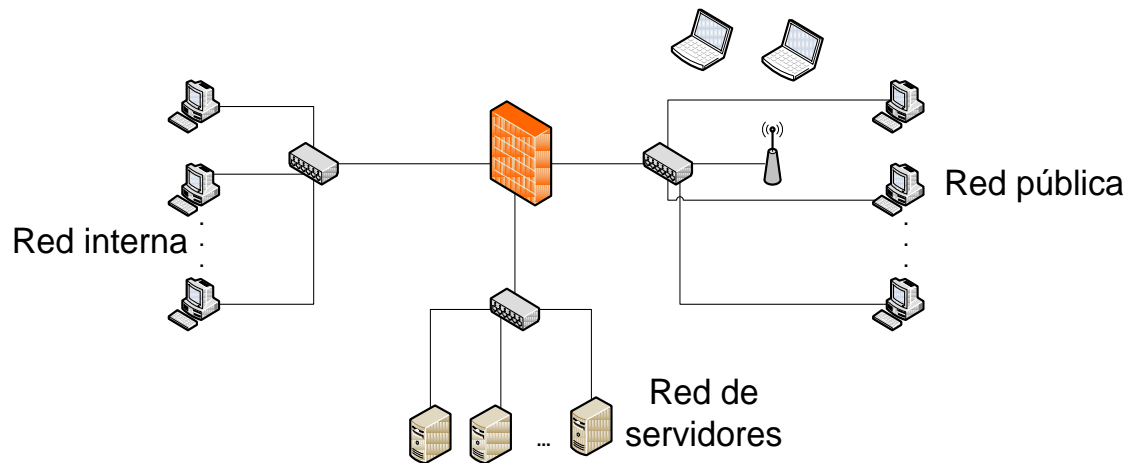
Luego que la política de seguridad ha cumplido con lo que se tenía establecido, o ya no es necesaria, esta etapa involucra el retiro del sistema de las políticas por cuestiones de rendimiento y eficiencia.

4.3. Soluciones de vulnerabilidades

A continuación se darán soluciones prácticas a la mayoría de problemas encontrados en las redes analizadas:

- Sobre los puntos de red libres: es necesario tener un control sobre todos los tomas de red que se estén utilizando, y aquellos que no estén en uso deben de desconectarse del *patch panel*. Para la aplicación de esto, es necesario que todos los puntos estén debidamente identificados.
- Aplicación de DMZ: el uso de los servidores en la misma red, donde se encuentran los usuarios de la red, los hace vulnerables a ataques internos. Para reducir este tipo de riesgos, es necesaria la implementación de un *firewall*, que permita dividir la red tanto de servidores, clientes internos y clientes externos.

Figura 19. **Propuesta de uso de zona desmilitarizada (DMZ)**



Fuente: elaboración propia.

- Sobre acceso a red pública: para la red pública en especial en el uso de la tecnología WiFi, se debe hacer uso de los mecanismos de seguridad que estas poseen, aun siendo esta red pública, se debe prevenir que cualquier persona no permitida ingrese a la red.

Tabla VI. **Recomendaciones de seguridad inalámbrica**

Descripción	Complejidad
Cambiar la contraseña que trae por defecto	Baja
Usar mecanismos de encriptación WEP/WPA/WPA2 (en nivel de seguridad están escritos de menor a mayor)	Alta
Cambiar el nombre de difusión (SSID)	Baja
Cambio de claves continuamente	Media
Desactivar DHCP, a menos que sea necesario	Alta

Fuente: elaboración propia.

- Revisión de puertos: se debe realizar un escaneo de los puertos que contengan los servidores y únicamente dejar habilitados aquellos que van a servir; deben cerrarse todos los demás, debido a que cada puerto abierto hace más vulnerable al sistema.
- Inyecciones SQL: este tipo de vulnerabilidades consiste en ingresar en los campos de los formularios de las páginas web que deben ser evaluados por el sitio, textos que complementen o modifiquen las sentencias SQL, definidas en las reglas del negocio.

Ejemplo:

```
<?php
$query = "SELECT * FROM usuarios WHERE usuario='{$_POST['usuario']}' AND password
='{$_POST['password']}';
mysql_query($query);
?>
```

Si no se realiza una revisión de los datos enviados, se puede ingresar lo siguiente:

```
<?php
$_POST['usuario'] = 'pepe';
$_POST['password'] = "" OR "=";
?>
```

Lo que daría como resultado una sentencia SQL como esta:

```
SELECT * FROM usuarios WHERE usuario='malo' AND password="" OR ""
```

Lo que daría como resultado que cualquier individuo logre ingresar a cualquier sistema, sin necesidad de una autorización.

La solución a esta debilidad, es aplicar la función que es parte de la librería mysql para php, que anulará todos los caracteres que pueden perjudicar:

```
string mysql_real_escape_string ( string cadena [, resource id_enlace] )
```

La solución al problema es:

```
<?php
$_POST['usuario'] = mysql_real_escape_string($_POST['usuario']);
$_POST['password'] = mysql_real_escape_string($_POST['password']);
?>
```

- Vulnerabilidad XSS: es una de las vulnerabilidades web más comunes, se produce habitualmente cuando no se validan correctamente los datos ingresados por el usuario que posteriormente son mostrados en una página, permitiendo la inyección de código “no deseado” (Javascript o VBScript).

La solución de esto, es similar a la de inyección de SQL se debe verificar toda la información que es ingresada por los usuarios a las páginas.

- También puede aplicarse la función de php strip_tags para eliminar todas las etiquetas, también elimina el código html.
- Sobre la visualización de directorios del sitio web: este tipo de vulnerabilidad deja de ser una amenaza, cuando los permisos de lectura, escritura y ejecución son debidamente aplicados, no permitiendo a personas no autorizadas el acceso a ningún dato.
- Sobre contraseñas: se recomienda que los usuarios cambien sus contraseñas frecuentemente, y que el sistema no permita utilizar la misma en repetidas ocasiones.
- Sobre los gestores de contenidos: es importante mantener actualizado el motor de gestor de contenidos para prevenir las vulnerabilidades con que estos cuentan.
- Sobre las peticiones GET: este tipo de vulnerabilidades, es fácil eliminarlas cambiando los métodos de petición en los formularios por POST en lugar del método GET.
- Prevenir ataques DOS: el ataque DoS tiene como objetivo bloquear o interrumpir algún servicio, para este caso el servicio web.
- Para prevenir este tipo de ataques es necesario el uso de la instalación de módulos adicionales en los servidores.

4.3.1. Apache

Este servidor para la prevención de ataques DOS necesita la instalación del módulo mod_evasive.

4.3.1.1. Configuración de Apache:

- DOSHashTableSize #: indica el tamaño de la tabla donde almacenaremos los datos de los clientes.
- DOSPageCount #: indica el máximo número de peticiones en el intervalo definido después para una URL específica.
- DOSSiteCount #: igual que el anterior, solo que aplica para todo.
- DOSPageInterval #: indica el intervalo de medida para una URL específica.
- DOSSiteInterval #: indica el intervalo de medida para todo el sitio.
- DOSBlockingPeriod #: indica el tiempo, en segundos, que va a estar bloqueada esa IP.
- DOSWhitelist #ip o dominio: indica ciertos dominios o IPs a los que no se quieren que se deniegue nunca el servicio.
- DOSEmailNotify: envía un mail a una cuenta de correo cada vez que se deniega el servicio a una IP.

- DOSSystemCommand: cada vez que se deniegue el acceso a una IP, ejecutará un comando en el sistema.

Una regla importante en cualquier sistema para reducir los riesgos es mantener los sistemas actualizados.

CONCLUSIONES

1. Un buen sistema de seguridad debe contener análisis que cubran todos los niveles de seguridad (físico, red, aplicación, usuario y sistema operativo), con el objetivo de prevenir el mayor número de amenazas posibles.
2. El costo de un sistema de seguridad nunca debe superar el valor de lo que se esté protegiendo, y se debe garantizar que el costo de *hackear* el sistema sea más elevado que lo protegido, para reducir la motivación del atacante.
3. Existe una gran cantidad de delitos informáticos, sin embargo, muchas veces ocurren accidentes de parte de usuarios que no han sido bien instruidos, y estos no pueden catalogarse como delitos.
4. A pesar de que los delitos informáticos afectan a todo el mundo, se hace imposible la creación de leyes internacionales que puedan reducir o erradicar estos, debido a que en la mayoría de las ocasiones, leyes de países vecinos son contrarias, por lo que hace complicado la creación de un estándar.
5. La aplicación de políticas de seguridad puede traer muchos beneficios a la organización, pero si estas no son bien aplicadas o analizadas, pueden crear conflictos dentro de la organización.

6. Un análisis exhaustivo de los riesgos a los que se enfrenta la organización puede llevar a minimizar los impactos de estos; sin embargo, en la mayoría de las ocasiones no pueden ser gestionados todos los riesgos, debido a que el costo que involucra tener una seguridad total es un precio que las organizaciones no están dispuestas a cubrir; el problema se da cuando alguna vulnerabilidad genera pérdidas aún mayores, se lamentan en no haber invertido un poco más en seguridad.
7. Existe un gran número de herramientas que los administradores de red pueden utilizar para detectar vulnerabilidades y poderlas corregir, lastimosamente es mayor el porcentaje de personas que utilizan estas herramientas con el objetivo de explotar dichas vulnerabilidades.
8. En la gestión de riesgos no se pueden tratar a los mismos de igual manera; se deben establecer listas de prioridad para atender a aquellos que puedan causar más daño.
9. La inversión en un sistema de seguridad siempre es recomendable, pero no se debe olvidar el factor humano, que si no es educado para que interactúe con los sistemas, siempre será la principal amenaza; una amenaza que es difícil de apreciar y reducir.

RECOMENDACIONES

1. Los gerentes de seguridad informática, deben brindar a las compañías un buen sistema de seguridad que pueda protegerlos y prevenir el mayor número de amenazas posibles.
2. A los gerentes financieros se les recomienda invertir en la seguridad de la información, debido a que es el activo más valioso con que cuenta la empresa.
3. El personal del área de las tecnologías de información y telecomunicaciones deben capacitar al personal que utilizará a los sistemas, para prevenir que los ataques provengan de fuentes internas.
4. Las personas encargadas de generar leyes para prevención y control de los delitos informáticos, deben buscar consensos internacionales para poder atacar a estas personas y aplicar sanciones correspondientes.
5. Los forenses de informática, deberán realizar un análisis exhaustivo de todo el entorno de los sistemas, para prevenir la mayor cantidad de ataques y reducir el riesgo de que la información sea dañada.
6. Los administradores de red, deben utilizar varias herramientas para analizar sus sistemas y descubrir vulnerabilidades, antes que personas con malas intenciones lo hagan y puedan explotarlas.

7. Los oficiales de seguridad deben realizar un estudio sobre la aplicación de políticas de seguridad informática, para prevenir conflicto entre las diversas aplicaciones de la empresa.

8. Los administradores de sistemas, siempre deben establecer prioridades para combatir los riesgos presentes en la organización, porque el costo de combatirlos todos puede ser muy elevado.

BIBLIOGRAFÍA

1. BEJERANO RAMÍREZ, Egil Emilio; AGUILERA RODRÍGUEZ, Ana Rosa. Los delitos informáticos. *Tratamiento internacional, en contribuciones a las ciencias sociales* [en línea]. Málaga, España: Juan Carlos Coll, mayo de 2009.
<http://www.eumed.net/rev/cccss/04/rbar2.htm>. ISSN: 1988-7833.
[Consulta en: 22 de diciembre de 2010].
2. BERENGUELA CASTRO, Alfonso Antonio; CORTÉS COLLADO, Juan Pablo. *Metodología de medición de vulnerabilidades en redes de datos de organizaciones* [en línea]. Dirección: Raúl Astorga Barrios, Chile: INACAP, 2006.
<http://seguinfo.zzl.org/tesis/medicion-vulnerabilidades.zip>.
[Consulta: 19 de diciembre de 2010].
3. CHIARAVALLOTI, Ricardo; LEVENE, Alicia. *Introducción a los delitos informáticos, tipos y legislación* [en línea]. delitosinformaticos.com.
[ref. 2 de diciembre de 2002] Disponible en Web:
<http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml>.
4. GAMBA, Jacobo. *Panorama del derecho informático en América Latina y el Caribe* [en línea]. Santiago de Chile: CEPAL, 2010.
<http://www.eclac.org/ddpe/publicaciones/xml/8/38898/W302.pdf>.
[Consulta: 20 de diciembre de 2010].

5. GARCÍA GUTIÉRREZ, Daniel. *Metasploitable: entorno de entrenamiento de seguridad informática*. No. 67, Polonia: Linux Plus Magazine, 2010. 50 p. ISSN: 1732-7121.
6. GARZARO GUILLÉN, Manuel. *La importancia de la definición de políticas de seguridad de la información en la empresa*. Trabajo de graduación de Ing. en Informática y Sistemas. Guatemala: Universidad Rafael Landivar, Facultad de Ingeniería, 2005. 105 p.
7. GAVARRETE, Ana Cristina. *Seguridad informática en las empresas para la protección de datos*. Trabajo de graduación de Ing. en Sistemas. Guatemala: Universidad Mariano Gálvez, Facultad de Ingeniería, 2004. 116 p.
8. HALL, Andrés. *Delitos informáticos reconocidos por Naciones Unidas* [en línea]. Argentina, [ref. 10 de octubre de 2007] Disponible en Web: <http://policiaonline.wordpress.com/2007/10/10/delitos-informaticos-reconocidos-por-naciones-unidas>.
9. HOWARD, John D. *An analysis of security on the internet 1989-1995* [en línea]. Pittsburgh, Pennsylvania: Carnegie Institute of Technology, Carnegie Mellon University, 7 de abril 1997. <http://www.cert.org/archive/pdf/JHThesis.pdf>. [Consulta: 20 de diciembre de 2010].
10. HOWARD, Patrick D.; TRIPTON, Harold F.; KRAUSE, Micki. *The security policy life cycle: functions and responsibilities. Information security management handbook. 6a ed.* Boca Raton, Florida: Aurebach Publications, 2007. 3150 p. ISBN: 978-0-8493-7495-1.

11. HUERTA, Antonio Villalón. *Seguridad en Unix y redes versión 2.1* [en línea]. Cuenca, España, 2002.
<http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf>.
[Consulta: 18 de diciembre de 2010].
12. KISSEL, Richard. *Glossary of key information security terms* [en línea]. Gaithersburg: NIST, 2010.
<http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf>. [Consulta: 19 de diciembre de 2010].
13. MARTÍNEZ, Antonio. *Convergencia: Borrmart.es*. [en línea] 2005.
http://www.borrmart.es/articulo_redseguridad.php?id=1794
[Consulta: 12 de febrero de 2010.]
14. MURILLO CANO, Sandra Rocío. *ASIS: Diseño y aplicación de un sistema integral de seguridad informática para la UDLA* [en línea]. Dirección: Dr. Antonio Sánchez Aguilar. Cholula, Puebla: Universidad de las Américas, mayo de 2001.
<http://seguinfo.zzl.org/tesis/sistema-seguridad-informatica.zip>.
[Consulta: 22 de diciembre de 2010].
15. NAVA GARCÉS, Alberto Enrique. *Análisis de los delitos informáticos*. México: Porrúa, 2005. 118 p. ISBN: 970045605X.
16. SAN MIGUEL CARRASCO, Rafael. *Metodología de desarrollo web seguro basado en formación a medida*. No. 152, Red Seguridad. Madrid: COIT, 2005. 101 p. ISSN: M-23.295-1978.

17. STONEBURNER, Gary; GOGUEN, Alice; FERINGA, Alexis. *Risk management guide for information technology system* [en línea]. Special publication 800-11, Gaithersburg, Maryland: National Institute of Standards and Technology, 2002.
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
[Consulta: 20 de diciembre de 2010].