INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS CUERNAVACA

TECNOLÓGICO DE MONTERREY®

DEFINICIÓN DE UN PROCEDIMIENTO PARA LA REALIZACIÓN DE AUDITORÍA EN SEGURIDAD INFORMÁTICA

Presentado por:

VLADIMIR VENIAMIN CABAÑAS VICTORIA

Sometido al Programa de Graduados en Informática y Computación en cumplimiento parcial con los requerimientos para obtener el grado de:

MAESTRO EN

ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Asesor:

Dr. Jesús Arturo Pérez Díaz

Cuernavaca, Morelos. Noviembre de 2005

DEFINICIÓN DE UN PROCEDIMIENTO PARA LA REALIZACIÓN DE AUDITORÍA EN SEGURIDAD INFORMÁTICA

Presentado por:
VLADIMIR VENIAMIN CABAÑAS VICTORIA

Revisada y Aprobada Por:

Dr. Jesús Arturo Pérez Díaz

Profesor e Investigador

Departamento de Electrónica ITESM, Campus Cuernavaca.

Asesor de Tesis

Dr. José Martín Molina Espinosa

Profesor e Investigador.

Departamento de Ciencias Computacionales ITESM, Campus Ciudad de México.

Sinodal

M.C. Francisco Alejandro González Horta

Profesor e Investigador

Departamento de Ciencias Computacionales ITESM, Campus Cuernavaca.

Sinodal

Dedicatorias

A mis padres:

Jorge Alberto Cabañas Cienfuegos y Lucía Victoria Muñoz

Por el apoyo incondicional que me han brindado durante toda mi vida.
Por el amor y el cariño demostrado en cada minuto de mi existencia.
Por ser mis padres, los mas maravillosos del mundo.

A mi hermano:

Pável Alexei Cabañas Victoria

Por ser ejemplo de tenacidad y lucha.
Por enseñarme que siempre se puede mejorar.
Ningún gemelo sería mejor.

A Gaby:

Gabriela Edith Balam Chi

Por todo su amor.
Por estar junto a mí en este camino tan hermoso que es la vida.
Por existir.

Agradecimientos

Dr. Jesús Arturo Pérez:

Por haber confiado en mí para la realización de esta tesis.

Por compartir sus conocimientos de manera desinteresada.

Por su preocupación para llevar a buen término este trabajo.

Dr. José Martín Molina Espinosa y MC. Francisco González Horta

Por sus observaciones y aportaciones en la revisión final de la presente.

Por su participación en la realización de una mejor tesis.

Catedráticos del ITESM

Por ampliar el mundo del conocimiento y mostrarlo ante mi.

A mi Familia.

A mis padres y a mi hermano.

A mis tíos: Julia, Bertha, Eufracia y Horacio.

A todos mis tíos.

A todos mis primos.

Gracias a todos por ser una gran familia.

A mis amigos y compañeros de la maestría:

Gaby, Lendy, Luis, Mode, MaryGo, Fito, Myrna y Ade

A cada uno de ellos, por hacer de esta etapa una gran experiencia de vida.

Gracias.

Resumen

El presente trabajo se ha desarrollado para proporcionar un procedimiento básico para la realización de auditorías en seguridad informática, específicamente en el área de redes con arquitectura cliente-servidor, este procedimiento se puede extender a diversas áreas de los sistemas de información y puede profundizar en cada uno de los elementos evaluados dentro de una organización.

En este procedimiento se han propuesto puntos de evaluación en materia de seguridad informática, importantes para determinar el nivel de fiabilidad del sistema en general, dejando en claro que cada práctica debe desarrollarse de acuerdo a las características propias de la organización y de su sistema de información.

Los elementos que se consideraron para el desarrollo del procedimiento auditor se dividen en dos categorías: la seguridad física y la seguridad lógica. Dentro de la seguridad física están presentes las políticas de seguridad física, el acceso físico a los componentes de hardware y al recinto de servidores. Por parte de la seguridad lógica se consideraron los aspectos de seguridad en el acceso, en el perímetro y en el canal.

La operatividad del procedimiento se basa en la implementación de diversos recursos que permiten el desarrollo de la labor auditora como: herramientas de software, cuestionarios, listas de verificación, etc. que hacen posible exhibir de manera sistemática los resultados obtenidos.

Para llevar a cabo el desarrollo de este procedimiento, se hizo un análisis de diversas metodologías de carácter libre, para el desarrollo de auditorías en tecnologías de información, de las cuales se tomaron los aspectos más importantes y se enfocaron al tema de seguridad informática, basándose en un estándar de código abierto para su diseño.

Se implementó dicho procedimiento para evaluar los resultados y la puesta en marcha de una auditoría dentro de la red interna en el Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Cuernavaca; esto permitió recopilar información relevante en el tema de seguridad informática, para definir una serie de medidas que permitan minimizar los riesgos y las probabilidades de fallos en la red interna a causa de acciones malintencionadas o descuidos.

C O N T E N I D O

Capítulo 4 Procedimiento de Auditoría

Capítulo 5 Caso Práctico

Lista de Figuras

Lista de Tablas

Capítulo 1 Introducción

La administración de tecnologías de información, se sirve de diferentes disciplinas para llevar a cabo su función primordial de administrar de una manera eficiente y eficaz, los recursos informáticos en las organizaciones, dentro de estas disciplinas se encuentra la auditoría.

El procedimiento de auditoría en la administración proporciona la constante vigilancia y la evaluación que requieren las actividades ya sea de tipo financieras, comerciales operativas etc., para el monitoreo de la eficiencia y la eficacia en el cumplimiento de sus objetivos. Generalmente, dicha evaluación consiste en una revisión metódica, periódica e intelectual de los registros, tareas y resultados de la empresa, con lo cual se busca medir y diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones. [MUÑOZ02].

En la implementación de auditorías se encuentra un área en particular que es tema central de la presente investigación: La auditoría en seguridad informática.

La auditoría en seguridad informática es, un recurso que proporciona elementos específicos para obtener información acerca de la fiabilidad de los sistemas informáticos de una organización, el análisis de los resultados obtenidos contribuye a realizar la planeación de acciones dirigidas a minimizar los riesgos y percances que pueden presentarse durante la operación de los sistemas.

La importancia que cobra la auditoría en seguridad informática, radica en el hecho de tener no sólo una “imagen” del nivel de seguridad que guardan en un momento determinado los sistemas informáticos, sino además, el poder evaluar, analizar y estudiar de manera sistemática, el grado de vulnerabilidad del sistema en general, esto es muy útil si se quiere lograr cierto nivel de fiabilidad en la operación del sistema informático, por parte de los administradores de los sistemas.

Para lograr una evaluación de manera sistemática, es necesario identificar elementos que nos permitan clasificar los principales componentes de un sistema informático, como es el sitio donde se encuentran sus principales componentes, el hardware, mecanismos de protección y monitoreo, así como también sus sistemas operativos, el software en general, accesos, recursos compartidos, etc.

También debe tomarse en cuenta, el gran desarrollo de las comunicaciones y la integración que caracteriza a los sistemas de información de la actualidad y, la consecuencia de generar una situación en la que el tráfico de datos y su uso masificado, ha incrementado las transacciones vía sistemas que hoy son consideradas parte de los activos de las empresas y, que son blanco de ataques informáticos. [ANONIMO,00]

1.1 Definición del Problema

La auditoría en informática es la revisión técnica especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes, ésta realiza la función de un examen crítico, que no implica necesariamente la preexistencia de fallas en los sistemas informáticos y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de una organización. [MUÑOZ02]

En este sentido, la auditoría se convierte en un recurso mas de las organizaciones para llevar un control estricto de lo que sucede en un momento del tiempo dentro de su infraestructura tecnológica informática.

Los sistemas de Información mal diseñados, mal implementados o que de alguna manera no corresponden a una configuración óptima, representan un grave peligro para la organización, éstas ya no pueden depender de software y hardware con altos niveles de vulnerabilidad, por consiguiente, es necesario realizar auditorías en materia de seguridad informática, como una herramienta actualizada y periódica para la implementación de un mayor grado de fiabilidad en los sistemas informáticos.

Las herramientas y procedimientos para llevar a cabo una auditoría en seguridad informática, han venido experimentando una difusión amplía también, las compañías que antes se enfocaban en soluciones para antivirus, ahora están integrando soluciones que permiten detectar intrusiones, configurar cortafuegos personales, llevar un registro de las actividades en los sistemas y de alguna manera contribuyen a aumentar el control con respecto a la seguridad informática.

Todo lo anterior, aunado a la realidad que se experimenta en el campo de la informática en donde es cotidiano encontrar hechos que ponen en riesgo la seguridad de los sistemas de información como: s*niffing*, fraudes electrónicos, *spoofing*, *hacking ataques de DoS* y un largo etc., permite deducir que es muy importante la cultura en seguridad informática y sobre todo, la puesta en marcha de revisiones y la práctica de auditorías.

De otra forma, la ausencia de auditorías en el área de seguridad en las organizaciones, permitiría en cierto grado que sean blancos fáciles de ataques no sólo de espionaje, sino también de delincuencia y terrorismo en sus sistemas de información.

Destacar la importancia que tiene la auditoría en seguridad informática como una herramienta que ayude a los administradores, usuarios y propietarios de la información en los sistemas computacionales de una organización, es una tarea que debe cobrar relevancia en la administración de sistemas de información.

Actualmente existen varias definiciones de métricas, parámetros y procedimientos para la auditoría informática, que proporcionan herramientas para que las organizaciones no comprometan del todo el nivel de la seguridad de sus sistemas informáticos. Lamentablemente estos elementos son muy poco conocidos por la mayoría de las empresas y organizaciones, de tal manera que las probabilidades de fallas a causa de ataques se incrementan si los sistemas no se implementan de manera correcta.

Estas son sólo algunas razones que hacen evidente la necesidad de definir un procedimiento (objeto de la presente tesis), que permita por una lado, resaltar la importancia de practicar auditorías de seguridad en los sistemas informáticos y por otro lado, que sirva como base para la realización de éstas, siendo convenientes de implementar para organizaciones que deseen obtener un mayor nivel de seguridad del que presentan actualmente.

1.2 Propuesta

Este procedimiento de auditoría, se propone como un recurso que debe colaborar a mejorar la eficacia y la eficiencia de la organización informática, proporcionando elementos suficientes que permitan tomar decisiones adecuadas y brinden un mayor nivel en la protección de sus activos y recursos. Se orientará a dos aspectos fundamentales en la seguridad informática: la seguridad física y la seguridad lógica.

Dentro de la seguridad física, el procedimiento determinará los elementos que pueden comprometer el buen funcionamiento de los componentes del sistema informático, como causas naturales y humanas, accesos no autorizados, vigilancia y una adecuada administración *in situ*.

En la parte lógica, se analiza el grado de vulnerabilidad en los sistemas operativos, así como en los servicios y mecanismos de protección existentes, como cortafuegos, proxy, seguridad en puertos, uso de protocolos seguros, uso de redes privadas virtuales, contraseñas, actualizaciones, y el uso de aplicaciones para corrección de errores conocidos (*hotfix*) así, como la existencia de sistemas que detecten intrusos y aplicaciones destinadas a la escucha y análisis del tráfico en una red.

1.3 Objetivo General

Definición de un procedimiento, para la realización de auditorías de seguridad en sistemas de información, basados en arquitecturas cliente-servidor, dentro de entornos distribuidos que contemple la seguridad física y lógica.

1.4 Objetivos Particulares

- Destacar la importancia y las implicaciones de una auditoría, en seguridad informática dentro de las organizaciones.

- Análisis de políticas para implementar seguridad de área, con el fin de establecer un procedimiento que permita incrementar su nivel de seguridad.

- Análisis para la auditoría de seguridad lógica. Para definir un procedimiento que, permita obtener información referente a la seguridad lógica y, que permita desarrollar e implementar acciones para obtener un mayor nivel de seguridad.

- Elaboración de una guía práctica para realizar una Auditoría de Seguridad en Sistemas Informáticos.

- Aplicación del procedimiento auditor en un caso práctico, que se realizará en las instalaciones de la red del ITESM, Campus Cuernavaca.

1.5 Alcances - Limitaciones

La complejidad y el alcance de un proyecto de esta naturaleza, en la que se pretende definir un procedimiento auditor de sistemas informáticos en el área de seguridad es enorme y extenso, por tal motivo, el presente se avocará en las siguientes áreas:

1.5.1 Alcances

- Auditoría de la seguridad física. El objetivo es evaluar las políticas, procedimientos y prácticas, para evitar las interrupciones prolongadas del servicio de procesamiento de datos e información, considerando:

  - Políticas de seguridad.
  - Seguridad del sitio
  - Revisiones periódicas del sitio
  - Planes de prevención ante contingencias

- Auditoría de la seguridad lógica:

  - Acceso

    - Seguridad en el sistema operativo.
    - Contraseñas
    - Políticas de seguridad lógica

  - Canal

    - Redes Privadas Virtuales
    - Conexiones seguras

  - Perímetro

    - Cortafuegos
    - Proxy
    - Puertos Seguros
    - Vulnerabilidades
    - Detección de Intrusos

1.6 Organización de la tesis

- **Capítulo 1**. En este capítulo se describen los motivos para la realización de la presente tesis, definiendo los objetivos, tanto generales como particulares, así como los alcances y la justificación.

- **Capítulo 2.** Se presenta el panorama general de los diferentes tópicos, como la auditoría orientada a la seguridad informática, el papel del auditor y el impacto de la auditoría dentro del ambiente de la organización

- **Capítulo 3.** En este capítulo de hace un análisis de algunos procedimientos de auditoría, desarrollados por universidades y organizaciones sin fines de lucro.

- **Capitulo 4**. En este otro capítulo se describe el procedimiento resultado de la investigación, de los principales elementos de los sistemas de información, para llevar a cabo, una evaluación de su nivel de fiabilidad.

- **Capítulo 5**. Es desarrollado y puesto en práctica el procedimiento con los elementos descritos en el capítulo 4, tomando como organización objetivo, al Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Cuernavaca

- **Capítulo 6**. Se describen las conclusiones que arrojó la investigación, también son descritos los trabajos futuros.

- **Anexo A**. Contiene la descripción de las herramientas y software utilizados.

- **Anexo B**. Glosarios de términos.

Capítulo 2 Estado del arte

2.1 Introducción

El desarrollo de las tecnologías de información, ha tenido un auge exponencial dentro de diversas instituciones, tanto de carácter privado como del servicio público, también sin importar el tamaño que éstas tengan, están haciendo cada vez mayores inversiones en el área de informática y de telecomunicaciones, todo ello para dar respuesta a los avances que se generan en tecnología. Uno de los objetivos primordiales de los administradores de estas tecnologías, se basa en el aprovechamiento de las funcionalidades que éstas representan; es decir, existe una gran concentración en explotar los recursos informáticos que las organizaciones van adquiriendo; este hecho ha sido especialmente orientado a la implementación de estas tecnologías, recayendo la responsabilidad en los jefes del departamento de informática, quienes desarrollan diversas labores de administración que, a menudo, se centran en la instalación, configuración, diseño, implementación, desarrollo y mantenimiento de los diferentes componentes de los sistemas informáticos.

Todas estas actividades deben tener siempre en cuenta, un fenómeno que ha ido creciendo durante los últimos años*:* la seguridad informática. Los riesgos que implican los virus informáticos, los ataques, las intrusiones, la denegación de servicios, el espionaje etc., representan serias amenazas para el buen funcionamiento del departamento de sistemas computacionales de una organización, así como su sistema de comunicaciones (estrechamente ligado a su departamento de informática), y los datos e información que albergan. Actualmente, cada uno de estos elementos es considerado como parte de los activos de las organizaciones. La necesidad de toda organización de garantizar sus inversiones en este tipo de activos, sobre todo cuando crece la dependencia hacia ellos, ha potenciado la aparición de la Auditoría en Seguridad de Sistemas de Información como un servicio orientado a garantizar, no sólo la salvaguarda de estos activos, sino también la utilidad que éstos reportan.

Las organizaciones son cada vez más dependientes de sus redes informáticas y, un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes, es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día, habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse, las fallas de seguridad provenientes del interior mismo de la organización. [ArCERT 00]

2.2 Auditoría

La auditoría es un examen crítico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o a la empresa en general, consiste en una revisión exhaustiva sistemática y global que realiza un equipo multidisciplinario de profesionales de todas las áreas de la empresa, con el propósito de evaluar de manera integral el correcto desarrollo de sus funciones, conjuntos y relaciones de trabajo, así como sus procedimientos y comunicaciones utilizadas para alcanzar el objetivo institucional. [MUÑOZ02]

Así, la auditoría informática es:

a) Un proceso formal ejecutado por especialistas en el área de auditoría y de informática;
b) Actividades ejecutadas por profesionales de las áreas de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos informáticos. [HERNANDEZ, 00]

Para entender la auditoría de seguridad en sistemas informáticos, debemos definir algunos conceptos:

La auditoría informática es la revisión técnica especializada y exhaustiva que se realiza a los sistemas computacionales, *software* e información utilizados en una empresa, sean individuales, compartidos o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. [MUÑOZ02]

También abarca un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente de acuerdo con las normas informáticas y generales existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente. [QUINN]

La aplicación del conjunto de procedimientos y técnicas anteriores, contribuye al dominio de la empresa sobre el rubro de seguridad de sistemas computacionales, lo cual permitirá a la organización, tomar decisiones con respecto al nivel de seguridad, o en su defecto, sobre el nivel de vulnerabilidad que los sistemas computacionales presenten en un momento determinado.

La función auditora no tiene carácter ejecutivo, ni son vinculantes sus decisiones, queda a cargo de la organización tomar las decisiones pertinentes. La auditoría simplemente refleja en su informe final sugerencias y planes de acción para eliminar las disfunciones y debilidades detectadas.

2.3 Clases de auditoría

Por su forma de aplicación (Entidad que la realiza):

- Interna
- Externa

Por su área de aplicación:

- Financiera
- Contable
- Operacional
- De Sistemas

Especializadas en áreas específicas:

- Área médica
- Fiscal
- Laboral
- Sistemas computacionales

2.3.1 Auditoría interna

Es cuando la auditoría es realizada con recursos materiales y personas que pertenecen a la empresa auditada. La realiza un profesional de la auditoría cuya relación de trabajo es directa y subordinada a la institución donde aplicará la misma, con el propósito de evaluar el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por intención expresa de la empresa, es decir, que puede optar por su disolución en cualquier momento.

La principal ventaja de realizar la auditoría de manera interna radica en que perteneciendo el auditor a la empresa auditada, éste conoce integralmente sus actividades, operaciones y áreas, de esta manera su revisión puede ser más profunda y con resultados muy valiosos. La desventaja de este tipo de auditorías es que los resultados pueden verse afectados por la influencia de las autoridades de la empresa, es decir, existe la posibilidad de que el informe de evaluación se vea limitado y que no cumpla las expectativas puestas en ella. [MUÑOZ02].

2.3.2 Auditoría externa

Es cuando se realiza por personas afines a la empresa auditada; la auditoría es siempre remunerada, se presupone una mayor objetividad que en la auditoría Interna, debido al mayor distanciamiento entre auditores y auditados, que permite al auditor utilizar mayor albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las cuales hará la evaluación y por lo tanto, en la emisión de resultados. Generalmente este tipo de auditorías son ejecutadas por organizaciones que cuentan con gran prestigio dentro del ambiente profesional. Su principal ventaja radica en que el trabajo de la entidad auditora es totalmente independiente y libre de influencia por parte de los directivos de la compañía. [MUÑOZ02]

Una Empresa o Institución que posee auditoría interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

1. Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.

2. Contrastar algún Informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.

3. Servir como mecanismo protector de posibles auditorías informáticas externas decretadas por la misma empresa.

4. Aunque la auditoría interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas como para tener una visión desde afuera de la empresa.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o por encargo de la dirección o cliente

Dentro del área de los sistemas computacionales y debido al gran desarrollo que han tenido las tecnologías de información y con ello algunas áreas especializadas, encontramos necesidades específicas de evaluación para los diferentes niveles de operación y administración, por ejemplo: la auditoría a la gestión informática, auditoría a los sistemas de redes, auditoría a la seguridad informática, auditoría *outsourcing*, auditoría de *software*, auditoría de explotación, cada una de ellas dirigidas a necesidades específicas de evaluación y control dentro de la organización.

2.3.3 Auditoría informática de software

Se ocupa de analizar la actividad que se conoce como técnica de sistemas, en todos sus factores. La importancia creciente de las telecomunicaciones propicia que las comunicaciones, líneas y redes de las instalaciones informáticas se auditen por separado, aunque formen parte del entorno general del sistema. [MUÑOZ02].

2.3.4 Auditoría Informática de explotación

Esta auditoría consiste en analizar las diferentes secciones del sistema (orientados a los datos) y sus interrelaciones. Para ello tenemos la primera parte: Control de Entrada de Datos, en esta sección se analiza la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a alguna norma. [MUÑOZ02].

2.3.5 Auditoría Informática de desarrollo de proyectos o aplicaciones

La función de desarrollo es una evaluación del llamado Análisis de programación y sistemas. Así por ejemplo una aplicación podría tener las siguientes fases:

- Prerrequisitos del usuario y del entorno
- Análisis funcional
- Diseño
- Pruebas

Estas fases deben estar sometidas a un exigente control interno, en caso contrario, podría producirse la insatisfacción del usuario. La auditoría comprueba la seguridad de los programas en el sentido de garantizar que los que se ejecutan por la computadora sean exactamente los previstos. [MUÑOZ,02].

2.3.6 Auditoría informática de comunicación y redes

Este tipo de auditoría consiste en una revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando la evaluación de los tipos de redes, arquitectura, topología, protocolos de comunicación, las conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, funcionamiento y aprovechamiento, debe inquirir o actuar sobre los índices de utilización de las líneas contratadas con información sobre tiempos de uso y de no uso, y sobre todo ello, hacer una suposición de inoperatividad informática con el fin de prever posibles fallas.

Las actividades propias de este tipo de auditoría están orientadas en la misma dirección que la auditoría en seguridad informática: asegurar de alguna manera la funcionalidad de las comunicaciones (parte importante de la seguridad), por ello aunque se mencionen, en otro tipo de auditoría, éstas se encuentran estrechamente ligadas en un solo objetivo. [MUÑOZ02]

2.3.7 Auditoría de la seguridad informática

Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y su personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. Es también la revisión de los planes de contingencia y medidas de protección para la información, los usuarios y los propios sistemas computacionales, y en sí para todos aquellos aspectos que contribuyan a la protección y salvaguarda en el buen funcionamiento en el área de sistematización, sistemas de redes o computadoras personales, incluyendo su prevención y la erradicación de virus informáticos. [MUÑOZ02].

2.4 Aplicación de los tipos de auditoría informática

Cada uno de los diferentes tipos de auditoría están encaminados a áreas especificas dentro de las empresas, compañías o institutos en donde son aplicados, esto quiere decir que no todas las clases de auditoría son aplicadas, en algunas empresas se podrían dar todas, algunas o sólo una de las distintas auditorías, esto depende específicamente del tipo, giro y clase de la compañía o institución en cuestión. Veamos unos ejemplos:

2.4.1 Auditoría informática de explotación

Se aplica generalmente a compañías que dependen en un nivel muy alto de la entrada, captura, almacenamiento y tratamiento de los datos de por ejemplo sus clientes, socios, proveedores, etc. Para estas compañías es de vital importancia asegurarse que sus datos tienen un alto grado de confiabilidad y sus métodos de procesamiento son eficientes y eficaces.

2.4.2 Auditoría informática de desarrollo de proyectos o aplicaciones

Se dirige hacia empresas que tienen que ver con el desarrollo de software, específicamente ha sido diseñada para asegurar un alto nivel de calidad en el desarrollo y puesta en marcha de software nuevo.

2.4.3 Auditoría informática de software

Este tipo de auditoría aplica para todas las empresas que tengan sistemas de cómputo y que necesiten observar el cumplimiento de medidas encaminadas a asegurar el funcionamiento correcto de sus sistemas.

2.4.4 Auditoría informática de comunicación y redes

Si la compañía en cuestión posee una red, se comunica por medio de *módem*, *switches* o *routers*, si tiene una conexión hacia otros sistemas ya sean locales o externos entonces, esta compañía necesita de este tipo de auditoría para conocer el estado que guarda su configuración e instalaciones de sus redes. Es muy importante para las compañías estar comunicadas, pero también es muy importante hacerlo con un nivel de funcionamiento adecuado.

2.4.5 Auditoría de la seguridad informática

Los elementos computacionales (sistemas, periféricos, datos, equipo), son parte de los activos de cualquier compañía, éstos deben ser asegurados y, este tipo de auditoría se aplica a todas aquellas compañías que requieran garantizar un mínimo nivel de seguridad en su departamento de informática.

2.5 Seguridad informática

La seguridad, de acuerdo a la definición de la Real Academia de la Lengua, proviene de la raíz latina *securitas* que significa "cualidad de seguro", es decir, que se tiene conocimiento seguro y claro de algo. Dicho de un mecanismo o en este caso de un procedimiento aplicado a la seguridad de los sistemas computacionales, se refiere a: "que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente".

"La seguridad informática es la materia que se encarga de proteger los ordenadores, redes, sistemas informáticos y datos que en ellos se almacenan, de agentes externos o internos que pudieran dañarlos" [MIGUEZ03].

La definición anterior queda un poco corta, si se toma en cuenta que la seguridad informática no solo se limita a hardware y software, también le compete el uso adecuado de las instalaciones donde se manejan, es decir, implementar políticas de seguridad que regulen el tránsito del personal ,… contemplar medidas de contingencia y para salvaguardar la información. [AMADOR 01]

Debido a la complejidad actual de los servicios y sistemas de información y telecomunicaciones, cada vez es más difícil cubrir todas las vulnerabilidades de un sistema de un tamaño considerablemente grande, por lo que la seguridad de dichos sistemas y su capacidad para soportar situaciones en la que algún aspecto de la arquitectura de seguridad ha sido comprometida, son cuestiones críticas para una organización.

En ese sentido, los sistemas computacionales representan un complejo y variado concepto de la seguridad, ya que la seguridad informática nos define una serie elementos que deben considerarse seguros, a fin de evitar que fallen y por consiguiente que dejen de funcionar.

En función de esta definición, debemos dejar algo en claro: la seguridad informática es un fin que perseguimos, de esta manera alcanzamos un cierto nivel de fiabilidad, pero no queda exenta de algún evento, ya sea un ataque directo, una catástrofe, espionaje, robo, etc. Lo que se pretende al implementar mecanismos de seguridad es desarrollar un nivel de seguridad aceptable, minimizando de esta manera las probabilidades de fallos.

2.5.1 Consideraciones de la seguridad informática

¿Es posible garantizar al 100% de seguridad informática?, No, no es posible garantizar de alguna manera que los sistemas están protegidos en su totalidad, ¿la razón? diariamente encontramos fallas, vulnerabilidades de los sistemas operativos, de los protocolos, de hardware, todo esto en una lista que parece interminable, de la cual no podemos predecir su conducta.

Actualmente la seguridad informática se ha convertido en un tema de gran interés y que comienza a preocupar a los administradores de sistemas que desean mantener su operatividad. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados. [CANO 00]

La preocupación por la seguridad ha de ser continua y constante. Un sistema muy fiable pasa fácilmente a ser un sistema poco fiable si no se le presta la atención adecuada. Debido a la rápida evolución de la tecnología, son imprescindibles comprobaciones periódicas de la fiabilidad de las medidas implantadas, es decir, auditorías de seguridad.

2.5.2 Gastos e inversión

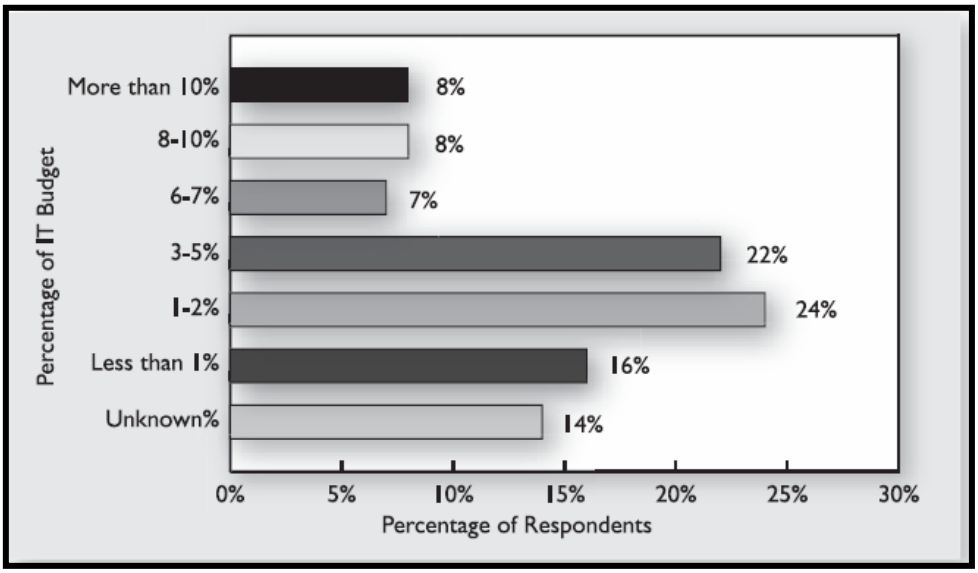

Figura 2.1 Porcentaje del gasto en TI, destinado a la seguridad informática **[CSI/FBI,04]**

Como se mostró en la figura 2.1, el presupuesto destinado a la seguridad en las tecnologías de información es considerablemente bajo en la mayoría de las instituciones, aunado a eso, la gráfica que se muestra en la figura 2.2 demuestra lo costoso de implementar un alto nivel de seguridad, lo que resulta casi inconcebible en términos de coste económico proteger, monitorizar, auditar y actualizar en tiempo real un sistema informático en su totalidad, es decir que sea 100% seguro, lo que se pretende realizar, y se hace en realidad, es estudiar las posibles debilidades conocidas de nuestras máquinas y sobre ellas aplicar las medidas de seguridad correspondientes [MIGUEZ03].

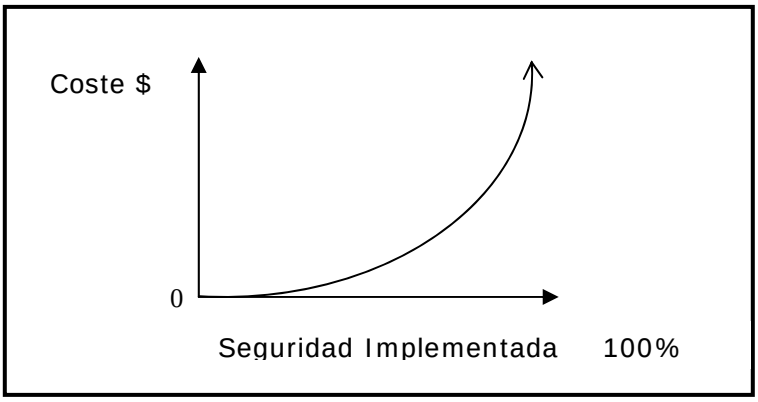

Figura 2.2 Implementación de Seguridad de acuerdo al costo económico

Aún cuando se observa que los recursos destinados a la seguridad todavía son bajos, "los resultados de la encuesta internacional de *Information Security Magazine* de abril 2004 (Briney 2004)", demuestran que "las inversiones en seguridad informática muestran una constante: fortalecimiento del perímetro de seguridad, actualización de infraestructura de seguridad y administración de la seguridad informática.

Mucha de esta inversión se concentra en aspectos de hardware, software y servicios, lo cual sugiere un concepto de seguridad informática orientado por el modelo de riesgos y controles, que si bien aporta elementos importantes para el mantenimiento de niveles de seguridad informática adecuados para la realidad de cada organización, limita la comprensión de eventos inesperados que generalmente no encuentran respuesta a los mismos y cuestionan el modelo de seguridad informática de la empresa." [CANO, 04]

2.6 Áreas de evolución en seguridad informática

Para desarrollar el procedimiento auditor, se propone una segmentación de las principales zonas (de acuerdo a las funciones que realice la empresa):

a) **Internet**: Zona que contiene todos los elementos que pueden ser accedido por cualquier usuario de Internet.

b) **Intranet**: Zona desmilitarizada (DMZ's) En caso de que exista, o que contengan elementos que sólo accederán usuarios de la empresa.

c) **Núcleo**: Esta zona debe ser tratada con especial atención y claramente diferenciada de Intranet. En esta zona sólo accederán ciertos usuarios de la Empresa y con los máximos controles de seguridad. Se encuentran aquí las bases de datos de facturación, personal, Investigación y Desarrollo, etc. [CORLETTI, 04]

2.6.1 Puntos de evaluación a considerar en seguridad informática

2.6.1.1 Seguridad Física

En un principio la seguridad física se refiere a la aplicación de barreras físicas y mecanismos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial, este tipo de seguridad se enfoca a cubrir las amenazas que pudieran ocasionar tanto el hombre como la naturaleza, es decir, va desde accesos físicos no autorizados hasta inundaciones, terremotos, etc.

Consideremos los principales aspectos de la seguridad física:

2.6.1.1.1 Amenazas naturales

Se engloban todos aquellos fenómenos naturales que el hombre no puede controlar y que pueden afectar nuestro sistema, entres ellos podemos destacar el fuego, el agua, un terremoto, un tornado, una tormenta, etc.

2.6.1.1.2 Amenazas humanas

La formarán todos aquellos riesgos que pueden afectar a nuestro sistema por parte de personas. Esas personas pueden ser ajenas a la empresa (personal de otra empresa, *hackers*, *crackers*, etc.) o personal de la propia empresa (personal descontento, accidentes involuntarios, etc.) [MIGUEZ03].

Dentro de estos dos grandes campos en las que dividimos las amenazas que en un momento determinado, pudieran interferir con el buen funcionamiento de los sistemas informáticos, presentaremos en el siguiente capitulo una descripción de los más comunes y, la manera en que éstos se pueden evitar en gran medida, para dar un sustento teórico a lo que se presentará como la práctica de la auditoría en esta área.

2.6.1.2 Seguridad Lógica

La seguridad lógica es propuesta en esta tesis como el conjunto de elementos de software y las políticas de que de algún modo, comprometen la integridad y la salvaguarda de los datos de las organizaciones, es decir, se centra en el sistema operativo, la correcta utilización de los recursos de software con los que cuenta la organización, así como también las políticas de grupos, tipos de usuarios, claves de acceso, privilegios, etc.

La seguridad en las comunicaciones implica una gran cantidad de elementos a considerar, las limitaciones del procedimiento auditor desarrollado durante la presente, se centrará en el monitoreo de la red, la gestión de los elementos de comunicaciones, las protecciones implementadas o por implementar como cortafuegos, la utilización de protocolos, seguridad en los puertos de comunicación, sistemas de detección de intrusos, etc., divididos en las siguientes clasificaciones

2.6.1.2.1 Seguridad de Acceso

Políticas para asignación de cuentas de usuario, grupos, contraseñas, robustez en los sistemas operativos. Administración de cada uno de estos elementos y una cultura de seguridad por parte de los administradores y usuarios.

2.6.1.2.2 Seguridad de Perímetro

Para prevenir ataques desde el exterior, básicamente este tipo de seguridad se base en cortafuegos, *proxys*, políticas de acceso, etc.

2.6.1.2.3 Seguridad de Canal

Para proteger los datos que viajan a través de los canales de comunicación, basándose en el cifrado de los datos, utilizando protocolos seguros y el uso de redes privadas virtuales.

2.7 Conceptos a considerar

Confidencialidad. Consiste en proteger la información contra la lectura no autorizada. Explícitamente incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para interferir otros elementos de información confidencial.

Integridad. Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo, sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y/o software.
- Causadas de forma intencional.
- Causadas de forma accidental
- Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

Autenticidad. En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

No repudio. Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

2.8 Procedimientos de auditoría en seguridad informática

Existe documentación acerca de la importancia de auditar sistemas en sus diferentes contextos, (de explotación, informática, de seguridad, de desarrollo de proyectos, etc.), pero los procedimientos para llevar a cabo la auditoría son muy pocos y muy generales. La razón: el procedimiento en todo su conjunto es un elemento considerado como activo para empresas de consultoría y *outsourcing*..

OSTMM2.0.pdf *Open-Source Security Testing Methodology Manual* es un estándar de metodología que sirve como base para la realización de pruebas de seguridad (*tests*), éstas son la base para la realización de auditoría informática, el cual contiene diferentes tópicos a reconocer durante la operación de la auditoría. Este documento está respaldado por la comunidad *Open source*.

Dentro del ámbito educativo, se encuentran algunos ejemplos de la investigación que se ha realizado, en relación con el tema de las auditorías en sistemas informáticos, por ejemplo de la Facultad de Filosofía, Especialidad en Informática en Guayaquil, Ecuador [NARANJO00] se ha propuesto un manual para la realización de auditoría en seguridad informática. Generalmente los procedimientos que se publican son el esfuerzo de personas vinculadas a entidades académicas, sin fines de lucro y con el sólo propósito de documentar un área que se mantiene de manera privada, por las compañías que las realizan.

2.9 Elementos para la realización de auditorías

Algunos de los medios que se utilizan para lograr estos los objetivos descritos

anteriormente son los siguientes:

- Cuestionarios. Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor, consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

- Entrevistas. La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a los cuestionarios.

- Listas de verificación. Como listas de preguntas sistematizadas, coherentes y clasificadas por materias para obtener información en orden previamente formulado.

- *Software*. Existente en el mercado para realización de pruebas sobre vulnerabilidades.

Técnicamente existen muchas variables dentro del entorno auditable, como se ha descrito anteriormente, éstas obedecen a necesidades especificas de la organización, pero existe algo muy importante del lado de la política de la empresa: la cultura de la auditoría, es decir, el término de auditoría lejos de ser visto como un examen, como una evaluación y una oportunidad de verificar el estado que guardan las operaciones y actividades de la organización y, que representan herramientas benéficas para los usuarios, son consideradas en muchas ocasiones como aspectos negativos en el desarrollo de las actividades de los empleados, ponen al descubierto las fallas cometidas de manera consiente o inconsciente y esto se refleja en una animadversión de un procedimiento, cuyo objetivo es el mejoramiento continuo de la eficiencia y eficacia de la empresa.

2.10 Papel de la auditoría de seguridad informática en la empresa

La profesión de la auditoría se rige por normas y criterios que generalmente son emitidos por asociaciones profesionales que aportan su experiencia, conocimientos y actualizaciones en dicha materia. [MUÑOZ02], pero esto no evita que normalmente se hagan adecuaciones de dichas normas dando respuesta a las características de la organización.

Entre los objetivos que se persiguen, al realizar una auditoría de seguridad informática se encuentran en primera instancia: la de realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la seguridad de su administración, de sus procesos, operaciones y resultados. La revisión debe ser especializada, debe tener objetivos claros, desde un punto de vista profesional y autónomo. Los resultados deben ser analizados, evaluados e interpretados de manera profesional, discreta y con un alto grado de ética por parte del auditor.

Los procesos que se realizan para llevar a cabo una auditoría, se ubican dentro de un área específica de la organización en donde se desea implementar y esto depende del tipo de auditoría que se pretende realizar, en este caso, se desarrolla en los departamentos de cómputo y en aquellas áreas de vital importancia para el funcionamiento del sistema en general (servidores, *hosts*, equipo de comunicación, personal, etc.)

La finalidad de la auditoría se centra en garantizar que los Sistemas de Información produzcan resultados fiables en plazo y costos aceptables y, que satisfagan las necesidades de los usuarios (integridad de los datos). Es decir, no se debe permitir bajo ninguna circunstancia que los sistemas fallen a causa de espionaje, alteración de datos, destrucción de los equipos o cualquier otro tipo de percance.

La operatividad es una función que consiste en que la organización y las máquinas operen, al menos en el nivel más bajo de funcionalidad. No se debe permitir detener la infraestructura informática, para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los Sistemas están operando, ese el principal objetivo: mantener tal situación.

El mejoramiento de los procedimientos, estándares y de la planificación, así como la colaboración en el diseño y actualización de las normas, son algunos de los otros objetivos que persigue la auditoría para garantizar, no solo la efectividad del sistema, sino también su eficiencia.

2.11 Papel del auditor informático

El papel de auditor debe estar encaminado hacia la búsqueda de problemas existentes dentro de los sistemas utilizados, y a la vez proponer soluciones para estos problemas. El auditor debe presentar las siguientes características (con gran capacidad) en los aspectos enunciados a continuación:

- Puntos de máxima eficiencia y rentabilidad de los medios informáticos, para emitir recomendaciones para el reforzamiento del sistema y el estudio de mejores soluciones, respondiendo a los problemas detectados en el sistema.

- Establecer requisitos mínimos, aconsejables y óptimos para su adecuación con la finalidad de que, cumpla para lo que fue diseñado, determinando en cada clase su adaptabilidad, su fiabilidad, limitaciones, posibles mejoras, costos.

- El auditor puede incidir en la toma de decisiones en la mayoría de sus clientes con un elevado grado de autonomía, dado la dificultad práctica de los mismos, de constatar su capacidad profesional y en desequilibrio de desconocimientos técnicos existente entre al auditor y los auditados.

- Deberá prestar sus servicios de acuerdo a las posibilidades de la ciencia y a los medios a su alcance con absoluta libertad, respecto a la utilización de dichos medios y en unas condiciones técnicas adecuadas para el idóneo cumplimiento de su labor.

- En los casos en que la precariedad de los medios puestos a su disposición, impidan o dificulten seriamente la realización de la auditoría, deberá negarse a realizar hasta que se le garantice un mínimo de condiciones técnicas que no comprometan la calidad de sus servicios o dictámenes.

- Cuando durante la ejecución de la auditoría, el auditor considere conveniente recabar informes de otros mas calificados, sobre un aspecto o incidencia que superase su capacidad profesional para analizarlo en condiciones idóneas deberá remitir el mismo a un especialista en la materia o recabar su dictamen para reforzar la calidad y viabilidad global de la auditoría.

- Deberá actuar conforme a las normas implícitas o explícitas de dignidad de la profesión y de corrección en el trato personal.

- El auditor deberá lógicamente abstenerse de recomendar actuaciones innecesariamente onerosas, dañinas, o que genere riesgo injustificado para el auditado e igualmente de proponer modificaciones carentes de bases científicas insuficientemente probadas o de imprevisible futuro.

Capítulo 3 Análisis de los procedimientos de auditoría

Dentro de este capítulo, se analizarán algunas metodologías que existen para llevar a cabo, auditorías de seguridad en sistemas informáticos, se pondrá especial énfasis en los aspectos mas importantes como lo es la metodología, las herramientas y el enfoque de cada uno de los procedimientos.

3.1 La auditoría informática dentro de las etapas de Análisis de Sistemas Administrativos. (Aieasa)

Este trabajo presenta una herramienta para supervisar el desarrollo de sistemas administrativos, como un buen ejemplo de lo que se está desarrollando dentro del ámbito de la administración de sistemas de información, y particularmente en las auditorías como una más de las herramientas administrativas. Este trabajo está enfocado a las diferentes etapas del desarrollo de sistemas, contempla a los sistemas informáticos como un todo y, se sumerge en los aspectos más importantes de cada una de las áreas que los componen.

3.1.1 Tipo de auditoría

El material presentado en este procedimiento de auditoría, no indica si la realización de la misma será interna o externa, aunque en el caso práctico, sugiere en su fase 1 la asignación del equipo auditor, que bien puede estar constituido por miembros de la organización o por un equipo consultor que haya sido contratado para ese fin. Por el área a la que esta orientado este procedimiento, está en la clasificación de auditoría de Sistemas y no contiene un área de especialización.

3.1.2 Metodología

El método que sigue este procedimiento de auditoría, pasa por las siguientes etapas:

- Alcance y objetivos de la auditoría informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.

La metodología que sigue este procedimiento de auditoría en algunas de las áreas, es el llamado CRMR <Computer resource management review> (Evaluación de la gestión de recursos informáticos). La naturaleza de una revisión como ésta, no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones más rápidas a problemas concretos y notorios. [QUINN]

En función de la definición dada, la metodología abreviada CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor informático encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión. [Quinn]

Por ello, de manera conceptual, la auditoría informática en general y la de Seguridad en particular, se desarrolla en seis fases bien diferenciadas:

Fase 0. Causas de la realización del ciclo de seguridad.
Fase 1. Estrategia y logística del ciclo de seguridad.
Fase 2. Ponderación de sectores del ciclo de seguridad.
Fase 3. Operativa del ciclo de seguridad.
Fase 4. Cálculos y resultados del ciclo de seguridad.
Fase 5. Confección del informe del ciclo de seguridad.

3.1.3 Áreas sometidas a la auditoría

Esta auditoría está enfocada a 5 áreas específicas: Explotación, Desarrollo, Sistemas, Comunicaciones y Seguridad. A continuación se presenta la división por áreas específicas y generales para el desarrollo de este procedimiento de auditoría. En la tabla 3.1 se muestra un esquema de las áreas a auditar.

Áreas Específicas	**Áreas Generales**			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

Tabla 3.1 Áreas Especificas de la Auditoría Informática.

Dentro del área de seguridad, se proponen 8 segmentos a evaluar:

- Segmento 1: Seguridad de cumplimiento de normas y estándares.
- Segmento 2: Seguridad de Sistema Operativo.
- Segmento 3: Seguridad de Software.
- Segmento 4: Seguridad de Comunicaciones.
- Segmento 5: Seguridad de Base de Datos.
- Segmento 6: Seguridad de Proceso.
- Segmento 7: Seguridad de Aplicaciones.
- Segmento 8: Seguridad Física.

3.1.4 Herramientas y técnicas

3.1.4.1 Entrevistas

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de dos formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad
- Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo.

El auditor informático experto, entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud, a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

3.1.4.2 Cuestionarios

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores, dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos.

El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias. Para esto, suele ser lo habitual comenzar solicitando el cumplimiento de cuestionarios preimpresos, que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

3.1.4.3 Listas de verificación (*checklist*)

El auditor profesional y experto, es aquél que reelabora muchas veces sus cuestionarios, en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir, que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para el cumplimiento sistemático de sus cuestionarios, de sus listas de verificación.

3.1.4.4 Log

Considerado como un historial que registra lo que fue cambiando y cómo fue cambiando en las actividades del sistema.

3.1.4.5 Ponderación y asignación de pesos

Es una técnica que es implementada durante la fase dos de este procedimiento de auditoría, consiste en las asignaciones de pesos a Secciones y Segmentos del área de seguridad que se audita, y se realizan del siguiente modo:

Pesos técnicos**.** Son los coeficientes que el equipo auditor asigna a los Segmentos y a las Secciones.

Pesos políticos**.** Son los coeficientes o pesos que el cliente concede a cada Segmento y a cada Sección del Ciclo de Seguridad.

Pesos finales. Son el promedio de los pesos anteriores. El total de los pesos de los 8 segmentos es 100. Este total de 100 puntos es el que se ha asignado a la totalidad del área de Seguridad, como podría haberse elegido otro cualquiera. El total de puntos se mantiene cualquiera que hubiera sido el número de segmentos. Si hubieran existido cinco segmentos, en lugar de 8, la suma de los cinco habría de seguir siendo de 100 puntos**.**

El establecimiento de valores (pesos técnicos, políticos y finales) en cada una de las secciones a evaluar, permite finalmente obtener un valor cuantificable que señala el nivel de seguridad que tiene un sistema de información al momento de realizarse la auditoría. En la tabla 3.2 (siguiente página) se muestra un ejemplo de asignación de los diferentes pesos.

Suma Peso Secciones = 20 (con independencia del número de Secciones consideradas)			
Secciones	Pesos Técnicos	Pesos Políticos	Pesos Finales
Secc1. Seg. Física de Datos	6	6	6
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
Total	20	20	20

Tabla 3.2 Ejemplo de asignación de valores en una matriz de riesgos

3.1.4.6 Otros

Este procedimiento menciona otras herramientas y técnicas como:

- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).

3.2 Auditoría de sistemas. (ADS)

Este trabajo realizado por el Ing. Alice Naranjo S., Profesor de la Universidad de Guayaquil Facultad Filosofía-Especialidad Informática de Ecuador, comienza con una descripción de los tipos y clases de auditoría, define los objetivos y la justificación para realizarla. Un aspecto importante de este procedimiento es el hincapié que hace en las medidas administrativas enfocadas a la seguridad, que pone de manifiesto la preocupación por la definición de un reglamento de políticas de seguridad organizacional como una de las herramientas efectivas en el control administrativo de sistemas de información.

3.2.1 Tipo de auditoría

De acuerdo a su forma de aplicación, este procedimiento de auditoría es interno, ya que se pretende realizar con miembros de la misma organización, por su área de aplicación se encuentra en la clasificación de Sistemas y por su área de especialización corresponde al tipo de Seguridad

3.2.2 Metodología

Lo primero que propone es una clasificación de controles, para prevenir, detectar y por último para corregir. Los primeros elementos que contempla son los controles de acceso tanto físico como lógicos, seguido de controles administrativos, y una serie de ejemplos prácticos para llevarlos a cabo. Esta metodología propuesta consiste en 4 etapas:

- Estudio preliminar.- Incluye definir el grupo de trabajo, el programa de auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el control interno, solicitud de plan de actividades, manuales de políticas, reglamentos, entrevistas.

- Revisión y evaluación de controles y seguridades.- Consiste de la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas criticas, Revisión de procesos históricos (respaldos), Revisión de documentación y archivos, entre otras actividades.

- Examen detallado de áreas criticas.- Con las fases anteriores el auditor descubre las áreas criticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcances y recursos que usará, definirá la metodología de trabajo, la duración de la auditoría, presentará el plan de trabajo y analizará detalladamente cada problema encontrado.

- Comunicación de resultados.- Se elaborará el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría.

El informe debe contener lo siguiente:

- Motivos de la Auditoría
- Objetivos
- Alcance
- Estructura Orgánico-Funcional del área Informática
- Configuración del *hardware* y *software* instalado
- Control Interno
- Resultados de la Auditoría

Finalmente, presenta 7 situaciones como caso práctico, para identificar las políticas de seguridad que evitarían en cierto grado los escenarios propuestos.

3.2.3 Áreas sometidas a la auditoría

Esta auditoría esta enfocada a 5 áreas específicas:

- *Hardware*. Definido por todos aquellos elementos que conformen el sistema informático, computadoras, microcomputadoras, ruteadores, *gateways*, etc.
- *Software*. Sistemas Operativos, Bases de Datos, Manejadores de bases de datos, Lenguajes de programación, Hojas de cálculo, Procesadores de palabras, Diseño Gráfico, Programas antivirus, Correo electrónico y Navegadores.
- Personal. Miembros de la organización, así como todas aquellas personas que se tengan contacto directo o indirecto con la misma.
- Datos. Como uno de los activos más importantes de toda organización.
- Instalaciones. Contempla mobiliario, instalaciones eléctricas, y todos aquellos elementos contenidos en el entorno informático.

3.2.4 Herramientas y técnicas

Este procedimiento no identifica elementos claves para la realización de la auditoría, es decir, no especifica las herramientas que deben utilizarse para llevarla a cabo, se limita a señalar una serie de acciones a realizar y utiliza controles descritos en la metodología de este procedimiento, en la siguiente figura se muestra un control, determinado por un código, las políticas generales a las que pertenece, la asignación de un responsable y el encargado de verificar el control. En la figura 3.2 se puede observar el documento que permite llevar un control sobre las políticas de seguridad en un entorno informático.

AREA O DIRECCION			
DEPARTAMENTO			
Código	POLITICAS GENERALES		Predecesor
Fecha de Vigencia	Ultima Revisión	Vto. Bno.	Vto. Bno.
		Cargo	Cargo

Tabla 3.3 Ejemplo de Controles de políticas en la auditoría de Sistemas.

Este tipo de herramientas son utilizadas para llevar a cabo una auditoría, y determinar las acciones que deben realizarse, sin embargo, estos controles siguen siendo utilizados para llevar un control periódico de las operaciones que se llevan a cabo.

3.3 Manual de auditoría de sistemas. (MAS)

Este manual de auditoría realizado por Oscar Toro, del Centro de Formación Técnica Diego Portales en Concepción Chile, es propuesto para desarrollar e implementar sistemas informáticos dentro de las organizaciones, es decir, su aplicación esta enfocada a guiar las diferentes etapas del software.

Está orientado a definir las etapas del desarrollo basado en una metodología estándar, que puede proporcionar un mayor nivel de seguridad en la implementación de sistemas comparado con sistemas que no siguen una metodología.

3.3.1 Tipo de auditoría

En este procedimiento, el personal es asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas; debido a esto, este procedimiento se clasifica en Interno, por su área de aplicación corresponde a Sistemas de Información, y no contiene un área de especialización.

3.3.2 Metodología

La metodología seguida en este procedimiento contempla las fases de:

- Investigación preliminar. Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización. Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas.

- Administración. Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar:

- A nivel del área de informática.

  - Objetivos a corto y largo plazo.
  - Recursos materiales y técnicos
  - Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
  - Fechas de instalación de los equipos y planes de instalación.
  - Contratos vigentes de compra, renta y servicio de mantenimiento.
  - Contratos de seguros.
  - Convenios que se tienen con otras instalaciones.
  - Configuración de los equipos y capacidades actuales y máximas.
  - Planes de expansión.
  - Ubicación general de los equipos.
  - Políticas de operación.
  - Políticas de uso de los equipos.

- A nivel de sistemas. Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

  - Manual de formas.
  - Manual de procedimientos de los sistemas.
  - Descripción genérica.
  - Diagramas de entrada, archivos, salida.
  - Salidas.
  - Fecha de instalación de los sistemas.
  - Proyecto de instalación de nuevos sistemas.

3.3.3 Áreas sometidas a la auditoría

Esta auditoría esta orientada a 6 áreas generales:

- Sistemas
- Diseño Lógico del Sistema
- Desarrollo del Sistema
- Control de Proyectos
- Control de Diseño de Sistemas y Programación
- Seguridad

Dentro del área de seguridad se encuentran las siguientes áreas específicas:

- Orden en el centro de cómputo
- Evaluación de la configuración del sistema de cómputo
- Seguridad lógica y confidencial
- Seguridad física
- Seguridad en la utilización del equipo
- Seguridad al restaurar el equipo
- Procedimientos de respaldo en caso de desastre

3.3.4 Herramientas y técnicas

- Entrevistas. El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

  - Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
  - Mediante entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

- Controles. La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al:

  - Suprimir u omitir datos.
  - Adicionar Datos.
  - Alterar datos.
  - Duplicar procesos.

Esto es de suma importancia en caso de equipos de cómputo que cuentan con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de los datos (uno de los usuarios debe ser el único responsable de determinado dato), con claves de acceso de acuerdo a niveles. En la figura 3.5 se muestra un ejemplo de control utilizado en la auditoría aplicada al desarrollo de sistemas.

PROGRAMA DE AUDITORIA EN SISTEMAS							
INSTITUCION_____ HOJA No._____ DE_____ FECHA DE FORMULACION_____							
FASE	DESCRIPCION	ACTIVIDAD	NUMERO DE PERSONAL	PERIODO ESTIMADO		DIAS HAB EST.	DIAS HOM. EST.
			PARTICIPANTE	INICIO	TERMINO		

Tabla 3.4 Ejemplo de Controles de políticas en la auditoría.

- Cuestionarios. Se utilizan para recabar información. Pertenecen al trabajo de campo del auditor y están dirigidos a personas específicas dentro del entorno organizacional:

3.4 Análisis de las metodologías

Como se puede observar en este capitulo, estas son solo algunas de las metodologías para llevar a cabo auditorías en sistemas de información, todos ellas con varias características en común, la primera de ellas es que todas pertenecen a esfuerzos de instituciones educativas o sin fines de lucro, por esa misma razón se encuentran disponibles en internet, ya que la información acerca de los que utilizan algunas compañías auditoras privadas no se encuentra disponible o publicada.

Otra característica que comparten es que están mas orientados a la auditoría desde el punto de vista puramente administrativo, dejando de lado aspectos técnicos que ayudan a materializar la auditoría, aterrizados en elementos concretos y en herramientas que pueden utilizarse. En la tabla 3.5 se muestra un resumen de las características mas importantes de los procedimientos de auditoría descritos en el presenta capítulo

En el caso de Aieasa, dentro del área de seguridad, define 8 segmentos a evaluar, sin embargo, no queda claro la forma en que se debe practicar la auditoría, ni están definidos los resultados que se deben obtener

Todos los procedimientos descritos en este capítulo, carecen de una especialización en el área de seguridad, en la cual debería existir un proceso más específico, que permita un mayor control sobre ésta y que proporcione información más precisa frente a posibles vulnerabilidades. Dentro del área de seguridad existen otras áreas más específicas como las comunicaciones que no están contempladas al cien por ciento dentro de las metodologías antes expuestas, y que en la actualidad representa un riesgo enorme el no practicar medidas de control sobre ellas.

			Áreas						Herramientas			
	Seguridad informática	Políticas de Seguridad	Física	Lógica	Comunicaciones	Inalámbrica	Otras Áreas	Complejidad	Software	Entrevistas	Listas de verificación	Monitoreo
Aieasa	*		*				*			*	*	*
Mas	*		*	*			*			*	*	*
Ads	*		*	*			*					

Tabla 3.5 Comparativa de los procedimientos de Auditoría.

En la mayoría de los procedimientos estudiados se aprecian omisiones de las herramientas o procedimientos específicos para evaluar algunas áreas, es decir, proporcionan información acerca de lo que debe auditarse, pero no especifican la manera en cómo debe hacerse. Por ello, es necesario desarrollar una guía que permita implementar las técnicas y herramientas propuestas en las diferentes metodologías, sumando también el software que permite descubrir vulnerabilidades y que ponen en evidencia los fallos a los que están expuestos los sistemas y con ello, a las organizaciones.

Otro elemento importante dentro de la práctica de auditoría es la presentación del informe final, es importante tener en cuenta el tipo de informe que se desea obtener, para que sirve, a quién le sirve, si es viable, y a quienes involucra. En el caso de Aieasa, por ejemplo, el informe final contiene un resumen de todos los pesos finales de las diferentes secciones que evalúa, con la finalidad de presentar un valor que refleje el estado general de la seguridad y de las otras áreas que participan. En el caso del procedimiento Ads, la presentación del informe final incorpora los resultados: problemas encontrados, los efectos de éstos y por último las soluciones propuestas.

Finalmente queda de manifiesto la preocupación de las instituciones tanto privadas como gubernamentales, por contar con sistemas que puedan considerarse seguros, en menor o mayor grado, dependiendo de los tipos de datos que se manejan dentro de sus organizaciones, del personal que labora con ellos, del giro de la organización y sobre todo de sus políticas de seguridad y administración con las que cuenten. Todos los procedimientos vistos en este capítulo ayudan de alguna manera a lograr este objetivo, de ahí la importancia de cada uno de ellos para las organizaciones que los apliquen.

Capítulo 4 Proceso de Auditoría

La auditoría en seguridad informática es un proceso que abarca diferentes áreas y se aplica en diversas etapas. Para el desarrollo del procedimiento auditor que se propone en el presente trabajo se tomarán las siguientes consideraciones:

- El sistema debe estar organizado por zonas de seguridad.
- Se definirán sus límites y puntos de acceso.
- Se integrarán las herramientas de detección y escucha.
- Se centrará la atención exclusivamente en servidores y elementos de red.

Se desarrollarán actividades tales como:

- Aplicación de la revisión y evaluación de los módulos de seguridad.
- Aplicación de entrevistas.
- Aplicación de listas de verificación para evaluar la seguridad del equipo
- Utilización de herramientas de software
- Análisis y evaluación de la información

Para la realización de la auditoría en seguridad informática se utilizará la siguiente metodología:

1) **Estudio inicial del entorno informático.** Para determinar el tipo de organización y sus necesidades de seguridad. Se proporcionará información acerca de la información general de la empresa, su ubicación geográfica, mapa de perímetro físico, características de la red, etc.

2) **Objetivos de la auditoría.** Determinar el nivel de vulnerabilidad y fiabilidad del sistema de información de la entidad auditada.

3) **Alcance de la auditoría.** Se definirán las zonas y las áreas que serán objeto de evaluación para determinar el alcance que tendrá el desarrollo del procedimiento auditor.

4) **Puntos de evaluación.** Definen los puntos a evaluar para determinar el nivel de vulnerabilidad. Se consideran los siguientes aspectos:

   Seguridad Física. Que permitirá conocer el grado de fiabilidad en la aplicación de barreras físicas y los procedimientos de control como medidas de prevención y contramedidas ante las amenazas a los recursos de hardware e instalaciones de áreas como:

- Departamento de cómputo.
- Sala de servidores.
- Red General (Estaciones de trabajo y cableado)

Seguridad Lógica. Este análisis permitirá conocer el grado de fiabilidad dentro del entorno lógico de la red en la organización. Se consideran los siguientes aspectos:

- Seguridad de Acceso
- Seguridad de Perímetro.
- Seguridad de Canal.

5) Herramientas

- Entrevistas
- Listas de verificación
- Software

6) Informe final

Elaboración del informe. Resultados descritos de manera sencilla y comprensible en redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la auditoría

4.1 Módulo 1 Descripción general de la empresa

Este módulo permite recabar información pertinente a la seguridad en general de la organización.

- Descripción de la empresa.
- Organigrama.
- Servicios
- Ubicación geográfica

La información en este punto, marca la pauta del desarrollo de la auditoría, de acuerdo a los datos recabados, será orientada la auditoría tratando de ser congruente con las necesidades (expresadas o no) de la entidad que requiere la auditoría.

La ubicación geográfica, así como la distribución de las instalaciones que conforman la organización, son referencias importantes para determinar los puntos físicos y los puntos de acceso al inmueble, que en algún momento representarían una debilidad o una fortaleza en cuestiones de seguridad física. El auditor debe conocer los puntos que podrían ser utilizados por intrusos o por personas malintencionadas, así como los lugares donde se pueden sustraer activos informáticos

4.2 Módulo 2 Zonas de seguridad

1. **Internet**: En esta zona se encontrará todo elemento que puede ser accedido por cualquier usuario de Internet.

2. **Intranet**: A esta zona sólo accederán usuarios de la empresa. Se pueden considerar también aquí a los socios y clientes, si los mismos están debidamente autenticados y registrados.

3. **Núcleo**: Esta zona debe ser tratada con especial atención y claramente diferenciada de Intranet. En esta zona sólo accederán ciertos usuarios de la Empresa y con los máximos controles de seguridad. Se encuentran aquí las bases de datos de facturación, personal, I+D, etc. [CORLETTI, 04]

4.3 Módulo 3 Puntos de evaluación

Una vez determinadas las zonas de seguridad, es necesario especificar los elementos que se van a evaluar, dividiéndolos de la siguiente manera:

4.3.1 Seguridad física

Esta sección del módulo permite evaluar las políticas, procedimientos y prácticas para evitar interrupciones prolongadas de servidores, hardware de comunicaciones y demás componentes del sistema informático frente a contingencias, tales como incendio, inundaciones, robo, sabotaje, disturbios, etc.

4.3.1.1 Revisión de las políticas de seguridad

Las políticas de seguridad computacional, son normas materializadas en documentos que describen la forma correcta y adecuada del uso de los recursos computacionales, las responsabilidades y derechos de los administradores y usuarios tienen, además de las medidas de contingencia para cada inconveniente computacional, en caso de catástrofes, donde prima salvaguardar la integridad de las personas y le sigue en jerarquía, salvaguardar la integridad de la información antes de cualquier maquinaria y equipo, claro está, sin dejar de lado la importancia que al hardware requiere, pero como última prioridad.

Este módulo permite hacer una evaluación de las políticas de seguridad en el área física.

Tareas a Realizar:

1. Obtener las políticas de seguridad física.
2. Examinar las políticas de seguridad.

Herramientas:

- Lista de verificación

Resultados Esperados:

- Evaluación e informe de las políticas de seguridad física

4.3.1.2 Plan de contingencia ante desastres

Es necesario que exista un plan que permita afrontar todos los riesgos posibles tanto para los equipos, como para las personas. Este módulo permite hacer una evaluación del plan de contingencia de la entidad.

Tareas a Realizar:

1. Obtener plan de contingencias.

Herramientas:

- Lista de verificación

Resultados Esperados:

- Evaluación del plan de contingencia

4.3.1.3 Revisión del área

Este es un método para evaluar y verificar las medidas de seguridad del área física.

Tareas a Realizar

1. Trazar mapa del perímetro físico, (área).
2. Trazar mapa de las medidas de protección físicas.
3. Trazar mapa de las rutas de acceso y/o métodos físicos

Herramientas a utilizar:

- Mapa de distribución de la entidad auditada.

Resultados Esperados:

- Mapa del perímetro físico
- Tipos de medidas de protección física
- Lista de áreas desprotegidas o insuficientemente protegidas

4.3.1.4 Contabilización de los principales componentes del sistema informático

Para enumerar el equipo principal con el que cuenta la entidad a auditar.

Tareas a Realizar

1. Enumerar dispositivos y tipos de control de acceso

Herramientas a utilizar:

- Listas de verificación

Resultados Esperados:

- Listas de dispositivos y control de acceso

4.3.1.5 Monitoreo

Para definir las áreas de acceso monitoreadas.

Tareas a Realizar

1. Definir los dispositivos de monitoreo
2. Trazar mapa de áreas monitoreadas y no monitoreadas
3. Examinar posibles ataques de denegación de servicio sobre los dispositivos de monitoreo

Herramientas a utilizar:

- Mapa
- Lista de verificación

Resultados Esperados:

- Tipos de monitoreo
- Lista de áreas monitoreadas
- Lista de áreas no monitoreadas

4.3.1.6 Instalación eléctrica

Este es un método, para evaluar la instalación eléctrica de los principales componentes de hardware del sistema de información.

Tareas a Realizar

1. Revisión de instalaciones eléctricas
2. Tierra física
3. Revisión de la protección contra descargas eléctricas

Herramientas a utilizar:

- Listas de verificación

Resultados Esperados:

- Lista de dispositivos suficientemente protegidos

4.3.1.7 Cableado

Esta sección se utiliza para evaluar el cableado que interconecta todos los dispositivos que componen la red.

Tareas a Realizar

1. Revisión del cableado

Herramientas a utilizar:

- Listas de verificación

Resultados Esperados:

- Estado del cableado general

4.3.1.8 Incendio y fuego

Sirve para determinar las medidas de prevención contra incendio

Tareas a Realizar

1. Revisión de instalaciones
2. Materiales inflamables
3. Revisión de dispositivos contra-incendios

Herramientas a utilizar:

- Listas de verificación

Resultados Esperados:

- Lista de medidas contra el fuego

4.3.1.9 Sistema hidráulico

Este es un método para evaluar el sistema de prevención de inundación y drenaje.

Tareas a Realizar

1. Revisión de instalaciones hidráulicas.

Herramientas a utilizar:

- Listas de verificación

Resultados Esperados:

- Estado del sistema hidráulico en general

4.3.2 Seguridad Lógica

En esta sección se hará la evaluación de los 3 principales aspectos lógicos de un sistema de información: seguridad de acceso (servidores), seguridad de perímetro y seguridad de canal.

4.3.2.1 Información de la red

Es una combinación de recolección de datos, obtención de información y política de control. Si se trata de una auditoría externa podría, no contar con dicha información, por lo tanto es necesario sondear y analizar. La clave es encontrar el número de sistemas alcanzables que deben ser analizados, sin exceder los limites legales de lo que se quiere analizar.

Tareas a Realizar:

Respuestas del Servidor de Nombres.

1. Recopilación de información acerca de los servidores.

Herramientas

- Software

Resultados Esperados:

- Nombres de Servidores
- Servicios que brinda
- Direcciones IP
- Mapa de Red

4.3.2.2 Políticas de seguridad

Tareas a Realizar

1. Obtener las políticas de seguridad lógica.
2. Examinar las políticas de seguridad.

Herramientas a utilizar:

- Listas de verificación

Resultados Esperados:

- Evaluación de las políticas de seguridad lógica.

4.3.2.3 Seguridad de Acceso

4.3.2.3.1 Evaluación de asignación de contraseñas

Es necesario evaluar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas, con distintas técnicas que dejen al descubierto la debilidad de los métodos utilizados en su asignación.

Tareas a Realizar

1. Realizar acciones de obtención de contraseñas por medio de diversas técnicas (ataques de fuerza bruta, ataques de diccionario)
2. Revisión de las políticas de tipos de usuarios y grupos en la asignación de contraseñas.

Herramientas a utilizar:

- *Software* de ataque de contraseñas

Resultados esperados:

- Obtención de contraseñas
- Lista de políticas para asignación de contraseñas

4.3.2.4 Seguridad de Perímetro

4.3.2.4.1 Cortafuegos.

El cortafuegos controla el flujo del tráfico de la red corporativa, la zona desmilitarizada (*DMZ*), e Internet. Opera en una política de seguridad y usa *ACL*'s (Listas de Control de Acceso). Este módulo está diseñado para asegurar que, sólo lo que debe estar expresamente permitido, puede ser aceptado dentro de la red, todo lo demás debe ser denegado.

Tareas a realizar:

- Verificar arquitectura del cortafuegos.
- Verificar las directivas del cortafuegos.
- Verificar si el cortafuegos cumple con *NAT*.
- Verificar que el cortafuegos esté haciendo detección de direcciones orígenes falsas.
- Verificar si el cortafuegos está filtrando el tráfico de la red local hacia afuera.
- Verificación de la configuración de las ACL
- Probar la ACL del cortafuegos en contra de las políticas de seguridad y en contra de la regla "Denegar Todo".

Herramientas a utilizar:

- Listas de verificación

Resultados esperados:

- Información del cortafuegos como servicio y como sistema
- Información de las características implementadas en el cortafuegos
- Perfil de la política de seguridad de la red a partir de la ACL
- Lista de los tipos de paquetes que deben entrar en la red
- Lista de tipos de protocolos con acceso dentro de la red
- Lista de protocolos que han entrado en la red
- Lista de rutas sin monitorizar dentro de la red

4.3.2.4.2 Sistemas de detección de intrusos. (IDS)

Este módulo está enfocado a evaluar las técnicas de detección de intrusos, analizando y determinando actividades anómalas, incorrectas y e ilegales, que se pueden estar aplicando a un sistema de información. La mayor parte de este módulo, no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS. Algunas de estas pruebas están relacionadas con ataques de ancho de banda, saltos distantes, y latencia que afectan al resultado de estas pruebas.

Tareas a Realizar:

1. Verificar el tipo de IDS.
2. Determinar rango de protección o influencia.
3. Determinar la técnica utilizada.

Herramientas a utilizar:

- Listas de verificación

Resultados esperados:

- Tipo de IDS
- Tipo de paquetes eliminados o no escaneados por el IDS
- Tipo de protocolos eliminados o no escaneados por el IDS
- Nota del tiempo de reacción y tipo del IDS
- Mapa de reglas del IDS
- Lista de alarmas perdidas del IDS

4.3.2.4.3 Búsqueda de vulnerabilidades

La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red. La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de actualización de los sistemas.

Tareas a Realizar:

1. Integrar en las pruebas realizadas los escáneres, herramientas de *hacking* y *exploits* utilizados actualmente.
2. Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.
3. Intentar determinar vulnerabilidades por tipo de aplicación y sistema.
4. Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
5. Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades.
6. Identificar todas las vulnerabilidades relativas a los sistemas operativos.

Herramientas a utilizar:

- Listas de verificación
- *Software*

Resultados esperados:

- Tipo de aplicación o servicio por vulnerabilidad
- Niveles de actualización de los sistemas operativos
- Listado de posibles vulnerabilidades de denegación de servicio
- Listado de vulnerabilidades actuales.

4.3.2.4.4 Escaneo de puertos

El escaneo de puertos, es la prueba invasiva de los puertos del sistema, en los niveles de transporte y red. En este módulo, se deben enumerar los servicios de Internet activos o accesibles.

Una vez que los puertos abiertos han sido identificados, es necesario llevar adelante un análisis de la aplicación que escucha tras dicho servicio. En algunos casos, más de una aplicación puede encontrarse detrás de un servicio, donde una aplicación es la que realmente escucha en dicho puerto y, las otras se consideran componentes de la aplicación que escucha. El siguiente paso es identificar el sistema mediante las pruebas sobre el sistema, con el fin de obtener respuestas que puedan distinguir su sistema operativo y su versión.

Tareas a Realizar:

1. Enumerar puertos abiertos, cerrados o filtrados.
2. Enumerar puertos por encima del 1024.

Herramientas a utilizar:

- *Software* de escaneo de puertos.

Resultados Esperados:

- Puertos abiertos, cerrados y filtrados
- Servicios activos
- Tipos de Servicios

4.3.2.5 Seguridad de Canal.

4.3.2.5.1 Conexiones seguras a servidores con SSL

SSL(*Secure Socket Layer*) es un protocolo que provee un canal de comunicación seguro, desde equipos de la red hacia servidores locales

Tareas a Realizar:

Verificar el uso del protocolo SSL, para comunicación segura en los entornos que así lo requieren.

Herramientas a utilizar:

- Listas de verificación

Resultados esperados:

- Evaluación de la comunicación por un canal seguro de la información, que así lo requiera.

4.3.2.5.2 Conexiones seguras a servidores con SSH

SSH (*Secure Shell*) Este protocolo sirve para acceder a máquinas a través de una red de manera segura.

Tareas a Realizar:

1. Verificar el uso del protocolo SSH para comunicación segura.
2. Verificación de la versión de SSH.
3. Actualización de las versiones

Herramientas a utilizar:

- Listas de verificación

Resultados esperados:

- Evaluación de la comunicación por un canal seguro de la información, que así lo requiera.

4.3.2.5.3 Conexiones seguras a través de redes privadas virtuales

Una red privada virtual, conecta los componentes de una red sobre otra red, permitiendo que el usuario haga un túnel a través de Internet u otra red pública, de tal forma que permita a los participantes del túnel, disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas

Tareas a Realizar:

1. Verificar el uso de redes privadas virtuales, para comunicaciones fuera de la intranet si es que existe un servicio o una necesidad de la empresa, que así lo requiera.
2. Identificación de los protocolos utilizados para la creación del túnel seguro.
3. Identificación de la tecnología implementada

Herramientas a utilizar:

- Listas de verificación

Resultados esperados:

- Evaluación de la comunicación por un canal seguro de la información, que así lo requiera.

4.4 Informe final

El informe final, es el documento resultado de la aplicación del proceso de auditoría. Debe contener la siguiente información:

a) El resultado de la evaluación por zonas.
b) El resultado de la evaluación final.
c) Resumen de los resultados obtenidos en cada uno de los módulos.
d) Recomendaciones.

4.4.1 Resultados

Los resultados deberán mostrarse de una manera sencilla, ayudándose de matrices de resultados y gráficos, que permitan dar una idea de la incidencia de los elementos que representan amenazas para la seguridad de la red informática, de acuerdo a las zonas previamente definidas.

El resultado de la evaluación final, debe contener un informe general, del estado que guarda el sistema previamente auditado.

4.4.2 Recomendaciones

Las recomendaciones deben definirse tomando en cuenta las siguientes características:

a) Viabilidad
b) Máxima prioridad
c) Costo (si aplica)
d) Complejidad

Las recomendaciones deben ser acordes a los resultados y apegados a la realidad, tomando en cuenta, la factibilidad que cada una de ellas represente.

La presentación de las recomendaciones se hará por cada una de las observaciones descritas, a partir de los eventos que se son considerados como un riesgo para la seguridad del sistema.

Capítulo 5 Caso práctico

Este capítulo, se muestra la aplicación del procedimiento para realizar auditorías propuesto en el capítulo 4, con el fin de ejemplificar el desarrollo de una auditoría en una organización; debido a la complejidad que una actividad de esta naturaleza implica, dicha auditoría será aplicada a una parte del sistema general. Ésta parte será determinada en el punto 5.2, denominado Zonas de Seguridad.

Módulo 1

5.1 Descripción general de la Empresa

La tabla 5.1 muestra información de la organización (Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Cuernavaca).

Información de la Empresa	
Nombre	Instituto Tecnológico y de Estudios Superiores de Monterrey. Campus Cuernavaca.
Domicilio	Paseo de la Reforma 182-A Col. Lomas de Cuernavaca C.P. 62589, Temixco Morelos, México. Tel. (777)329-71-00
Giro	Institución Educativa y de Investigación de carácter privado. Niveles de Preparatoria, Licenciatura y Posgrado (Maestría y Doctorado).

Información de la Empresa	
Servicios Informáticos:	▪ Administración de: • Servidores Windows NT, Windows 2000, Windows 2003, Linux (Fedora Core1) y Novell • Cuentas de correo electrónico • Aplicaciones Lotus Notes. • Sala de animación. ▪ Desarrollo de: • Aplicaciones multimedia. • Material de apoyo a cursos rediseñados. • Sistemas de información. • Bases de datos para cursos impartidos a través de LN. ▪ Telefonía: • Larga distancia. • Telefonía local (campus). ▪ Servicios para alumnos profesores y personal • Instalación y configuración de tarjetas de red • Configuración de impresoras del cec. • Instalación de software autorizado • Reinstalación de software y sistemas operativos de computadoras portátiles • Respaldo de información • Corrección de fallas de sistema operativo • Correo electrónico • Cuentas de ftp • Soporte técnico blackboard • Préstamos de tarjetas de red, cables y audífonos ▪ Servicios sólo para profesores y personal • Apoyo a aulas tecnológicas • Apoyo en eventos especiales • Solicitudes de hardware y software • Soporte técnico a áreas administrativas y académicas

Tabla 5.1 Características del Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Cuernavaca.

5.1.1 Ubicación geográfica

La figura 5.1 muestra el mapa general del inmueble, destacando la infraestructura de edificios, y sus principales accesos.

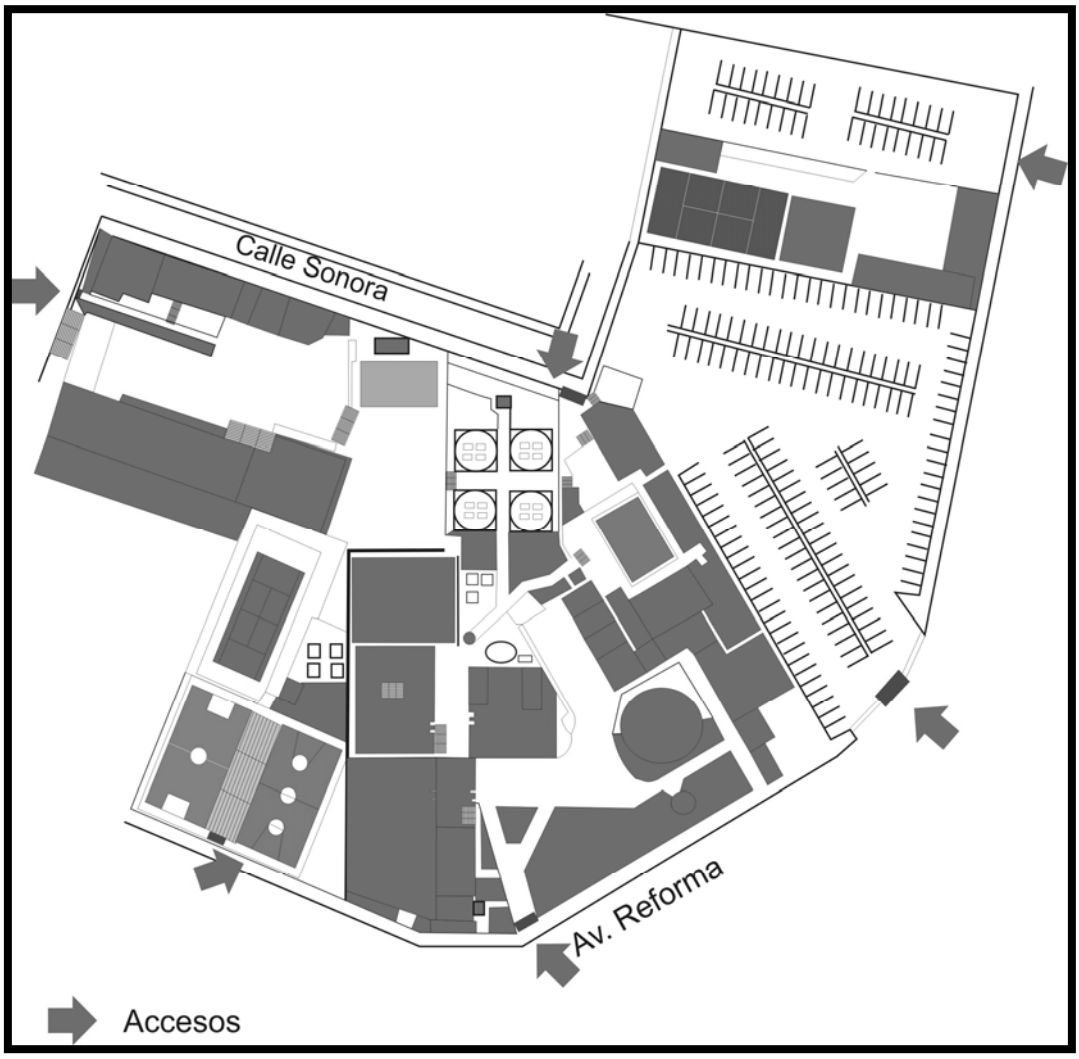

Figura 5.1 Mapa del Instituto Tecnológico y de Estudios Superiores de Monterrey

Módulo 2

5.2 Zonas de seguridad

Dadas las características de la red descritas en el apartado anterior, se definen las siguientes zonas de seguridad, que permitirá un mejor análisis y con ello, facilitará las actividades de la auditoría:

Zona 1: Intranet. Por la complejidad y característica de esta zona, se han definido 5 áreas:

> **Área 1**. *Zona de servidores*. Contiene los dispositivos e infraestructura que da soporte a los servicios ofrecidos por parte de la red del campus a nivel local.
>
> **Área 2**: *Red Cableada*. Incluye el *MDF* (*Main Distribution Facility*), los *IDF's* (*Intermediate Distribution Facility*) y el Nodo Principal (*POP*).
>
> **Área 3**. *Red inalámbrica*. Puntos de acceso. Cobertura, Calidad de Señal, Encriptación. Protocolos de autenticación.
>
> **Área 4**. *Red de servicios digitales*. Telefonía local y Larga Distancia
>
> **Área 5**. *Servidor de comunicaciones*. Conexiones simultáneas por módem y una línea telefónica.

Zona 2: **Núcleo**. Las áreas concentradas en esta zona obedecen a funciones específicas de empleados del Instituto, las cuales deben tratarse con especial cuidado. Algunos servicios son proporcionados directamente por la Rectoría del Instituto, por lo cual la aplicación de una auditoría rebasa los límites de la presente propuesta.

La auditoría que se aplicará, estará enfocada en el área 1 de la zona 1 (servidores). Esto debido a que realizar la auditoría en todas las áreas requiere de un lapso de tiempo considerablemente grande, además que se requeriría de un grupo multidisciplinario. Por tal motivo los puntos de evaluación quedan como a continuación:

Módulo 3

5.3 Puntos de evaluación para la seguridad informática

5.3.1 Seguridad Física

5.3.1.1 Revisión de las políticas de seguridad

No existen políticas de seguridad, sin embargo, existen medidas de seguridad implícitas y se listan a continuación:

- Existe un responsable de la seguridad informática del campus.
- Se ha definido el personal que tiene llaves para acceder a esta área.
- Se lleva a cabo un registro de acceso al área de servidores mediante una bitácora.
- Existe personal de vigilancia en la organización.

5.3.1.2 Plan de contingencia

No existe un plan de contingencia, pero se observan las siguientes medidas

- Los equipos se encuentran protegidos por unidades reguladoras de energía para evitar descargas eléctricas.
- Los equipos se encuentran conectados a fuentes de energía ininterrumpida (UPS) para evitar caídas de sistema por interrupción de la energía eléctrica.
- La temperatura en la sala de servidores se conserva a 18° C.
- Se cuenta con extintor especial para equipos electrónicos.
- El nivel de piso está elevado con respecto al piso general, para evitar en cierto grado que el equipo se moje en caso de una inundación moderada.
- Tierra física correcta
- Voltaje correcto
- Polarización de contactos correcto.

5.3.1.3 Revisión del área

- Mapa del perímetro físico.

La figura 5.2 muestra el mapa del perímetro físico del área de servidores. La ruta muestra el acceso desde la entrada principal, donde se encuentran elementos de seguridad que permiten el acceso previa identificación y autorización, pasando por el edificio donde se encuentra la Dirección General se accede al primer nivel del edificio con una puerta de vidrio sin cerradura. Al final de la sala se encuentra otro acceso, finalmente se debe acceder a la oficina del administrador de seguridad donde se encuentra el área de servidores tras una puerta de vidrio con cerradura.

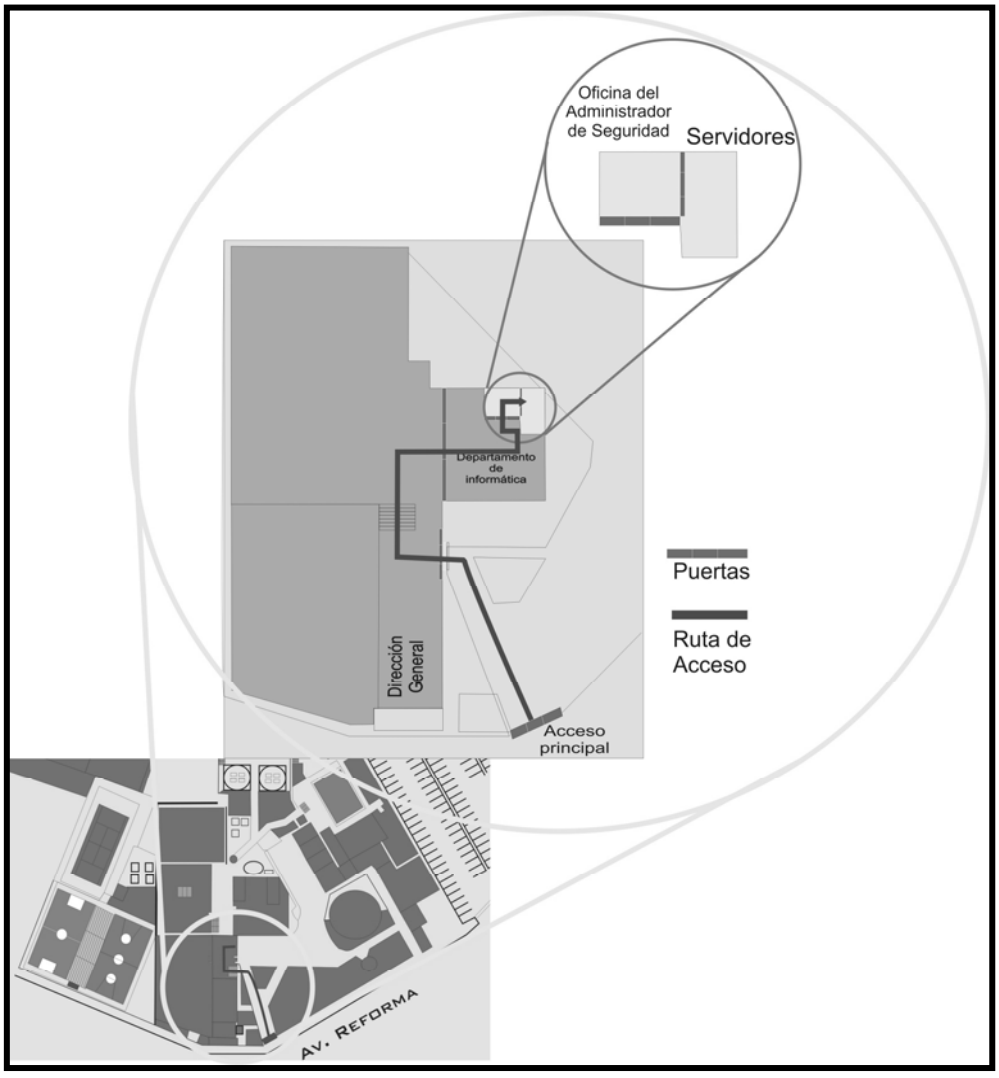

Figura 5.2 Mapa del perimetro fisico del área de servidores

5.3.1.4 Contabilización de componentes en el área de servidores

A continuación se muestran algunos de los componentes principales en el área de servidores, en la tabla 5.2 se muestran los equipos de redes y comunicaciones. En la tabla 5.3 se muestra el equipo de protección de energía para evitar caídas del sistema por falta de energía eléctrica así como evitar las variaciones bruscas de voltaje.

Equipo	Características
4 Switches	Cisco 4000
1 Switch 1 Hub	IBM 8274 (Para CSI Alumnos)
2 Acces Point	(informática) (cec planta baja)
2 Switches	3COM
10 Switches	Diversos fabricantes

Tabla 5.2 Equipo de Redes y Comunicación.

Equipo	Marca	Modelo
UPS	PROLYT	UPS3/1-10K-1P-SBS

Tabla 5.3 Equipo de energía eléctrica.

La tabla 5.4 muestra la información de sólo dos servidores ya que se ha omitido la lista completa con el fin de solo ejemplificar el procedimiento.

Equipo	Marca	Procesador
Morserver	IBM Netfinity 5000	Pentium III
Morcasa	HP NetServer LH II	Pentium Pro

Tabla 5.4 Servidores. Red ITESM Campus Cuernavaca.

5.3.1.5 Monitoreo

Áreas monitoreadas:

- No existen mecanismos de monitoreo para el área de servidores
- El área de servidores es visible ya que está separada solo por vidrio.

5.3.1.6 Incendio y fuego

- La instalación está hecha con materiales seguros.
- No existen materiales inflamables dentro del área de servidores
- Se cuenta con un extintor especial para equipos electrónicos.
- No cuenta con sistema detector de humo o fuego.

5.3.2 Seguridad Lógica

5.3.2.1 Información de la red

Los servicios principales para lo cual fue diseñada la red, es para dar soporte a los servicios de transmisión de datos de alta velocidad, conexiones telefónicas, servicios de red inalámbricos, y la conexión a través de enlaces dedicados. Existe además una intranet del Sistema Tecnológico de Monterrey, la cual da soporte a los servicios de biblioteca Digital y enlaces para sesiones académicas virtuales y lo referente a educación a distancia.

Características de la Red		
Tipo de Información	Datos, Voz y Video	
Tecnología WAN	ISDN Enlaces E1	
Redes	10.49.128.0 10.49.144.0 10.49.145.0 10.49.146.0 10.49.147.0 10.49.148.0 10.49.149.0 10.49.150.0 10.49.151.0 10.49.153.0	10.49.154.0 10.49.155.0 10.49.156.0 10.49.157.0 10.49.158.0 10.49.159.0 148.241.192.0 132.254.32.0 132.254.36.0 132.254.43.0 132.254.46.0
Protocolos	Ruteo: • OSPF • BGP Interconectividad: • TCP/IP. No ruteables: • NetBEUI • NetBIOS	

Tabla 5.5 Características generales de la Red del Campus Cuernavaca.

5.3.2.2 Diseño jerárquico de la red. (General)

En la figura 5.3 se muestra un panorama del diseño por capas de la red del campus, la capa central contiene básicamente dos ruteadores Cisco 3600, uno de ellos para realizar la conexión a Internet, mientras que el otro ruteador es utilizado con dos enlaces, uno de ellos con la compañía Alestra (microondas) y el otro con Telmex (Fibra óptica) para la intranet del Sistema TEC de Monterrey.

La capa de distribución, se basa en switch en el que se encuentran conectados los servidores de la red y, el PBX para los servicios de telefonía descritos en el punto anterior.

La capa de acceso está compuesta por un ruteador Cisco 4000 conectado a un grupo de *switches*, puntos de acceso (para la red inalámbrica) y concentradores que permiten la conexión directa a los usuarios de la red.

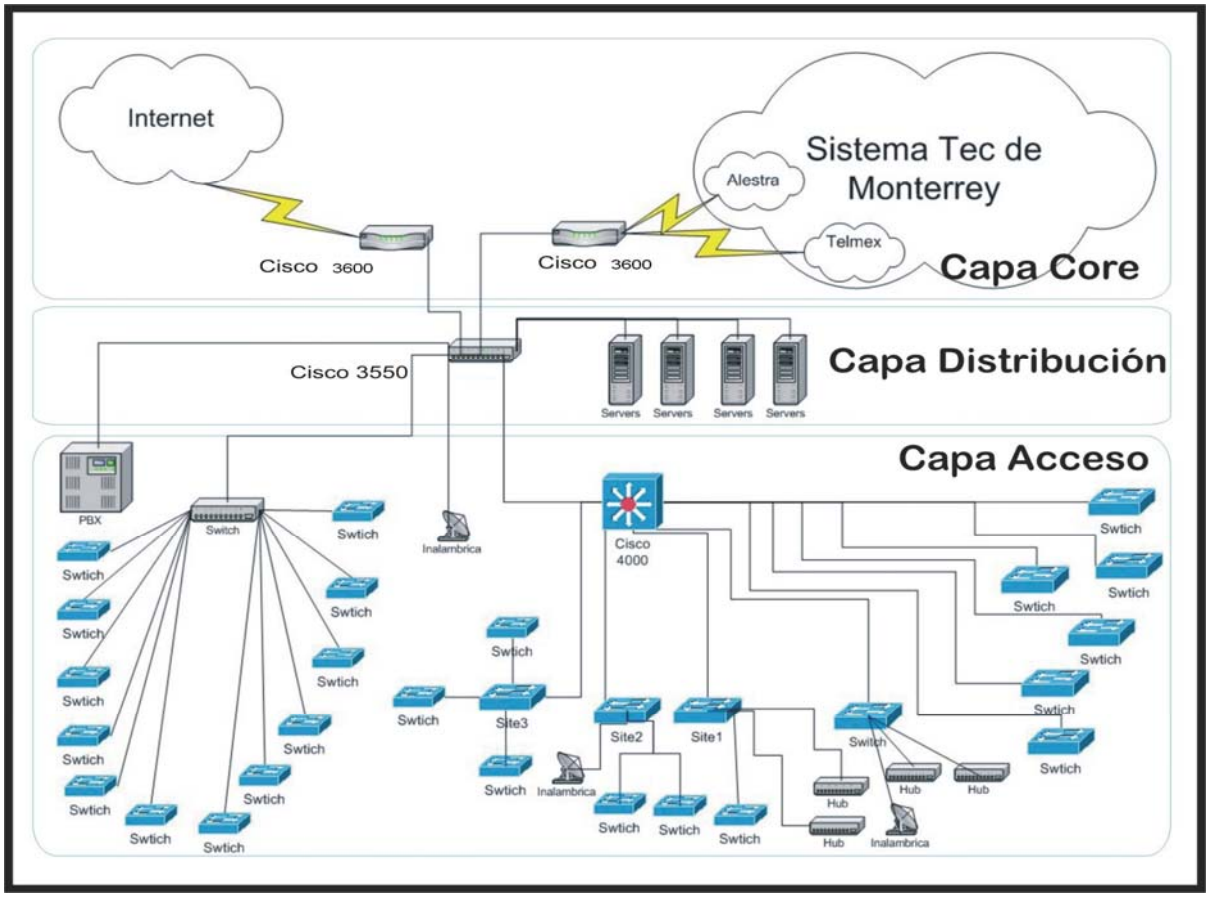

Figura 5.3 Diseño Jerárquico de la Red ITESM Cuernavaca.

5.3.2.3 Políticas de seguridad

La administración de los servidores carece actualmente de un documento que contenga políticas de seguridad. Sin embargo existen algunas medidas de seguridad dictadas por el área de Informática de la Rectoría de la Zona a la que pertenece el campus. Estas medidas hacen referencia a la aplicación de las actualizaciones en los sistemas operativos que se encuentran corriendo en los diversos servidores. También se proporciona el servicio de actualizaciones para el sistema de antivirus y el servicio de Active Directory para las cuentas de correo electrónico y servicios de impresión.

5.3.2.4 Seguridad de Acceso

Para llevar a cabo el procedimiento de auditoria se tomaron como ejemplo dos servidores de la red interna del ITESM, Campus Cuernavaca. A continuación se listan algunas de las características más importantes de los servidores mencionado anteriormente.

Dirección IP	Host	Sistema Operativo	Servicios	Dirección MAC
10.49.141.201	Morserver	Windows 2000	Controlador de Dominio Servidor de Licencias	00-50-DA-0B-FD-83
10.49.141.205	Morcasa	Windows Nt 4	Controlador de Dominio Servidor de Archivos Servidor Web	00-60-08-A8-D4-E1

Tabla 5.6 Características generales de los principales servidores de la Red ITESM Campus Cuernavaca.

5.3.2.4.1 Evaluación de asignación de contraseñas

Se realizó un análisis para evaluar contraseñas en los servidores Morserver y Morcasa. Se detectaron las siguientes condiciones que pueden comprometer la seguridad de los servidores.

Riesgo	Eventualidad	Descripción
Alto	Contraseñas idénticas al nombre de la cuenta	Se detectó que algunas cuentas presentan la contraseña idéntica al nombre de la cuenta.
Alto	Cuentas sin contraseñas	La cuenta de un usuario sin contraseña permite de manera fácil obtener acceso a los recursos de la red.
Medio	Cuenta “Administrator”	La cuenta del administrador de NT por default existe en uno de los servidores. Esta cuenta puede ser objetivo de ataques por fuerza bruta ya que no puede ser bloqueada al realizar demasiados intentos de conexión.
Medio	La contraseña nunca expira	Si la contraseña de un usuario nunca expira, se le puede permitir a un atacante calcular la contraseña con un ataque.
Bajo	No se puede cambiar la contraseña	Es recomendable definir que el usuario pueda cambiar su contraseña, de otra manera el cambio de contraseña sería mucho menos frecuente.

Tabla 5.7 Evaluación de las contraseñas en los servidores de la Red ITESM Campus Cuernavaca.

5.3.3 Seguridad de Perímetro

5.3.3.1 Cortafuegos

Existen dentro de la infraestructura de redes el ITESM Campus Cuernavaca dos aplicaciones distintas de cortafuegos:

- El primer esquema se basa en dos dispositivos de hardware que brindan el servicio de cortafuegos, estos equipos son Cisco Pix 515E y proporcionan protección para la comunicación de las aplicaciones del Sistema Tec.

- El segundo esquema es para la protección desde internet hacia la red interna del ITESM, Campus Cuernavaca, basado en listas de acceso implementadas en un *router* Cisco (3600).

    - Funciones:
        - Network Address Translation (NAT)
        - Stateful Packet Inspection (SPI)

- Las ACL´s fueron definidas por la rectoría del ITESM, con la política "*deny all*" y sólo se van agregando direcciones IP y puertos a discreción del administrador.

- Este tipo de cortafuegos es más rápido y transparente para el usuario, sin embargo presenta algunas fallas en la conexión a servidores Ftp fuera de la red interna.

5.3.3.2 Proxy

No se encuentra implementado ningún sistema de proxy para la conexión a internet. Lo que se traduce en falta de control y presenta también riesgos de seguridad por no administrar adecuadamente el contenido de las páginas y de los sitios que pueden visitarse.

5.3.3.3 Sistema de detección de intrusos

No se encuentra implementado ningún sistema para la detección de intrusiones (salvo la función de *spi* del cortafuegos). Esto permite que se puedan ejecutar aplicaciones para buscar vulnerabilidades sin ser detectados, así como programas que escuchen y monitoreen el tráfico en la red para obtener información que pudiera comprometer la seguridad informática.

5.3.3.4 Búsqueda de vulnerabilidades

La búsqueda de vulnerabilidades en los servidores arrojaron los siguientes resultados:

Riesgo	Tipo de Vulnerabilidad	Descripción
Alto	Servicios	Posible desbordamiento de búfer, Posibilidad de obtención de archivos, Startt/Stop del servidor web Ejecución de código arbitrario, Vulnerabilidades en Servidores Pop3, Versiones antiguas de Open SSH Posibilidad de sufrir ataques por medio de paquetes ICMP fragmentados Posibilidad de denegación de servicios, vulnerabilidades en los servicios de RPC, vulnerabilidades en el servidor de ColdFusion
Alto	NetBIOS	Posibilidad de enumeración de NETBIOS, por medio de Null Sesion.
Medio	Servicios	Múltiples vulnerabilidades del tipo CGI en el servidor ColdFusion
Bajo	Servicios	Servicios RPC, vulnerabilidad por ataque de fuerza bruta en el servidor de Netscape enterprise.

Tabla 5.8 Descripción de vulnerabilidades en los servidores de la Red ITESM Campus Cuernavaca.

La descripción completa de cada una de las vulnerabilidades encontradas en los servidores de la red interna, se encuentran en el informe final entregado a la dirección de servicios escolares, dirección de redes y telecomunicaciones y a la administración de recursos de cómputo y seguridad del ITESM, Campus Cuernavaca. El software utilizado para estas pruebas fueron: LANguard Network Security Scanner y Dragonsoft Secure Scanner.

5.3.3.5 Escaneo de puertos

La siguiente tabla contiene información de los puertos que se encuentran abiertos en los servidores Morcasa y Morserver, así como la relación con los servicios asociados a estos mismos puertos. La tercera columna muestra los troyanos más comunes que podrían utilizar dichos puertos.

Puerto	Servicio Asociado	Troyanos que podrían usar estos puertos
21	Ftp (file transfer protocol)	Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash
25	Smtp (simple mail transfer protocol)	Ajan, Antigen, Barok, Email Password Sender - EPS, EPS II, Gip, Gris, Happy99, Hpteam mail, Hybris, I love you, Kuang2, Magic Horse, MBT (Mail Bombing Trojan), Moscow Email trojan, Naebi, NewApt worm, ProMail trojan, Shtirlitz, Stealth, Tapiras, Terminator, WinPC, WinSpy
80	http (hyper text transfer protocol)	711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message Creator, Hooker, IISworm, MTX, NCX, Reverse WWW Tunnel Backdoor, RingZero, Seeker, WAN Remote, Web Server CT, WebDownloader
88	Kerberos	
110	Pop3 (post office protocol - version 3)	ProMail trojan
135	Rpc-locator (remote procedure call) location service	
139	Netbios – Session Service	Chode, God Message worm, Msinit, Netlog, Network, Qaz
389	Lightweight directory access protocol (LDAP)	
445	Microsoft-ds	
464	Kpasswd	
593	Http-rpc-epmap	
636	Ldapssl - ldap over ssl	
1026	NTERM	
1103	Xaudio	
2080	Wingate winsock redirector service	WinHole
3372		
3389	Microsoft Term server.2000/XP	
5376	Ms ftp	
5631	Pcanywheredata	
6400		The Thing
8000		
8080		Brown Orifice, RemoConChubo, Reverse WWW Tunnel Backdoor, RingZero

Tabla 5.9 Descripción de puertos en los servidores de la Red ITESM Campus Cuernavaca.

5.3.4 Seguridad de Canal

5.3.4.1 Conexiones seguras

Existen conexiones seguras utilizando *ssh,* de determinados *hosts* a equipos de comunicaciones (*switches* y *routers*) sin embargo, sólo se realizan en los equipos mas recientes y una gran cantidad de dispositivos no se conecta con algún mecanismo de protección.

Los principales servicios del sistema en la red interna, como el sitio web y los servicios de biblioteca, consulta de calificaciones, etc son proporcionado por el sistema Tec, en una conexión protegida por el esquema definido en el apartado de VPN's.

5.3.4.2 VPN's

Dentro de la red interna, no se han definido redes privadas virtuales. Existen redes privadas virtuales proporcionadas por los equipos Pix 515E de Cisco, éstas redes privadas permiten la comunicación segura con el sistema Tec de Monterrey y no son objeto del presente procedimiento.

5.4 Recomendaciones

5.4.1 Seguridad física

5.4.1.1 Revisión de las políticas de seguridad

Es necesario contar con políticas de seguridad para la administración de los servidores ya que representan una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos y garantizar la plena confidencialidad e integridad de los sistemas de información.

Algunas de las características que deben tener las políticas de seguridad son:

- Definición de su alcance, contemplando la facilidad de aplicación, y los elementos que en ella participen como los sistemas y personal que los utiliza
- Objetivos de la política y una descripción clara
- Responsabilidades de los administradores, y de los usuarios
- Requerimientos mínimos de configuración de servicios,
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

5.4.1.2 Plan de contingencia

- Es necesario contar con una guía que indique los procedimientos que deben ser seguidos por el personal de informática y los usuarios en caso de presentarse un evento que ponga en riesgo la seguridad de las personas y el buen funcionamiento y seguridad de los equipos de cómputo.
- También es necesario contar con un plan de contingencia ante la posibilidad de un ataque de tipo informático, que contemple algún mecanismo de recuperación, políticas de respaldo, puesta en marcha de servidores alternativos, etc.

Debido a que las organizaciones son diferentes, los ubicaciones geográficas son distintas, no puede existir una metodología fija para desarrollar un plan de contingencia genérico, sin embargo, un plan de contingencia debería contemplar al menos las siguientes 8 fases:

1) Inicialización del plan. Es el punto de comienzo, donde deberían definirse la meta del plan y los objetivos específicos que sean necesarios.

2) Gestión del riesgo y evaluación de las emergencias potenciales. La única manera de poder ordenar adecuadamente los procesos de recuperación es ordenando previamente los desastres que podemos sufrir, así como la evaluación de los mismos en términos de discontinuidad, así como su impacto técnico-económico en la organización.

3) Preparación para las posibles emergencias, identificado claramente los métodos de recuperación de copias de seguridad y otras técnicas de recuperación colaterales que pudieran ser necesarias.

4) Recuperación tras los desastres, donde deben quedar claramente definidos los pasos a seguir por los equipos de recuperación, especialmente en los casos donde haya riesgo de pérdida de vidas humanas.

5) Recuperación del negocio, ya que una vez aplicado el plan se pretende que el negocio como conjunto vuelva a la normalidad.

6) Pruebas del proceso de recuperación, en las que se pueden diagnosticar fallos y corregir deficiencias en las fases anteriores.

7) Entrenamiento del personal para el proceso de recuperación, ya que a fin de cuentas, el personal es el que ejecuta los planes.

8) Actualización constante del plan de recuperación, para mantener al día los procedimientos establecidos, así como la lista de emergencias potenciales y su valoración probabilística de riesgo. [HispaSec, 05]

5.4.1.3 Monitoreo

- El monitoreo representa una herramienta que permite vigilar el equipo de cómputo más importante e imprescindible del sistema en general. Se sugiere tomar en cuenta la posibilidad de establecer mecanismos de monitoreo en el área de servidores.

5.4.2 Seguridad Lógica

5.4.2.1 Seguridad de Acceso (Evaluación de asignación de contraseñas)

De acuerdo a los resultados obtenidos en la búsqueda de vulnerabilidades en las contraseñas, se sugieren los siguientes procedimientos para cada uno de los eventos de riesgo identificadas previamente

Nivel de Riesgo	Evento	Sugerencia
Alto	Contraseñas idénticas al nombre de la cuenta	Modificar las contraseñas utilizando una combinación de números y letras, también determinando un número mínimo de caracteres mayor a seis. [Common,05,01]
Ato	Cuentas sin contraseñas	Asignar contraseñas que brinden una mayor seguridad. [Common,05,02]
Medio	Cuenta “Administrator”	Renombrar la cuenta del administrador [Common,05,03]
Medio	La contraseña nunca expira	Deshabilitar la opción “Never expires” de la cuenta de los usuarios. [Common,05,04]
Bajo	No se puede cambiar la contraseña	Deshabilitar la opción: “User Cannot Change Password” para permitir al usuario cambiar la contraseña.

5.10 Vulnerabilidades en las contraseñas de los servidores de la red del ITESM C. Cuernavaca

5.4.2.2 Seguridad de Perímetro

5.4.2.2.1 Cortafuegos

La seguridad en el cortafuegos podría complementarse con el servicio de Proxy y el sistema para detectar intrusiones.

5.4.2.2.2 Proxy

Un sistema Proxy correctamente configurado en conjunto con el cortafuegos brinda una arquitectura de red bastante eficiente e incrementaría también el control del acceso a Internet desde la red interna. El administrador tiene contemplada su puesta en marcha para Diciembre de 2005.

5.4.2.2.3 Sistema de detección de intrusos.(IDS)

La implementación de un sistema para la detección de intrusos, permitiría detectar tipos de ataques que a veces puede "engañar" al cortafuegos, monitorizaría el tráfico en la red para verificar diferencias estadísticas del comportamiento normal de la red, registraría violaciones de seguridad, respondería ante una eventualidad anulando las sesiones y rechazando conexiones.

El sistema que se implemente debe presentar las siguientes características:

- Ser capaz de trabajar automáticamente para recoger, analizar y generar alertas oportunas.
- No debe afectar el *performance* del entorno donde se implemente.
- Debe poder adaptarse a los posibles cambios de la red.

5.4.2.2.4 Escaneo de puertos

La recomendación básica para puertos en servidores es: si una aplicación no lo está usando, si no es un servicio imprescindible, entonces el puerto no debe abrirse, es mejor bloquear el puerto, evitando así que alguna aplicación (troyano) se comunique con otro *host*, ya que cualquier servicio expuesto representa un punto de acceso potencial para intrusos. Si el puerto es usado por una aplicación, es recomendable también tener en cuenta el nivel de fiabilidad del servicio que está siendo usado por el puerto.

5.4.2.2.5 Vulnerabilidades

La descripción de cada una de las soluciones correspondientes a las vulnerabilidades encontradas en los servidores se encuentra en el informe de auditoría entregado a las respectivas autoridades del Campus.

Cada vulnerabilidad ha sido expuesta con su respectiva sugerencia para eliminar la probabilidad de que ésta se presente, algunas requieren que se actualice el software al que está asociada, en otras es necesario modificar la configuración de algunos archivos o del registro del sistema operativo en el caso de Windows.

5.4.2.3 Seguridad de Canal

Es necesario comenzar a implementar mecanismos que cifren la información que viaja a través de la red, ya se por medio de protocolos como SSH, así como la implementación de redes privadas virtuales.

Se puede comenzar con los equipos de telecomunicaciones (*switches* y *routers*), y paulatinamente a los *hosts* que ofrezcan servicios de conexiones.

Capítulo 6 Conclusiones

6.1 Conclusiones

Se ha definido un procedimiento básico pero extensible para realizarse de manera interna, con una metodología para comenzar analizando las características de la organización y definiendo dos aspectos esenciales de la seguridad informática: la seguridad lógica y la seguridad física así como la división por zonas y secciones la infraestructura de la red en general que permite de manera práctica poner en marcha un proceso de auditoría.

Para ello se analizaron algunos procedimientos para la realización de auditorías de los cuales se tomaron las características más relevantes para integrar un procedimiento que correspondiera con las necesidades de seguridad informática basándose en un estándar de código abierto.

Se puso de manifiesto durante el desarrollo de la investigación, la importancia que tiene realizar actividades encaminadas a proteger la información, destacando la auditoría como una herramienta de los administradores para tomar las decisiones que ayuden a asegurar la correcta operación de sus sistemas informáticos.

Se aplicó el procedimiento de auditoría en la red interna del ITESM Campus Cuernavaca, con el fin de evaluar su seguridad informática, los resultados mostraron que existen múltiples vulnerabilidades en diversas áreas, deficiencias en la implementación de algunos servicios y como resultado se propusieron las acciones a seguir para reducir el riesgo que éstas implican.

Se presentó un informe con los resultados y sugerencias a poner en práctica para elevar el nivel de seguridad en la red interna a la dirección de servicios escolares, a la coordinación de redes y telecomunicaciones y a la administración de recursos de cómputo y seguridad del ITESM Campus Cuernavaca.

Se puede concluir también que dentro de instituciones educativas y de investigación se encuentra una gran oportunidad para comenzar a reconocer la importancia de este tipo de herramientas en la administración de tecnologías informáticas, y que ellos se traduzca en actividades regulares dentro de las empresas, con el fin de mejorar la funcionalidad de los sistemas.

Es posible afirmar que no es posible obtener un 100% de seguridad informática, pero lo que si se puede hacer es tratar de minimizar los riesgos en la medida de las posibilidades de cada organización, dependiendo del costo que implica, del valor de lo que se quiere proteger, del tiempo y la preparación de los administradores.

6.2 Trabajos futuros

El procedimiento auditor propuesto presenta las limitaciones que implica el desarrollo producto de un esfuerzo personal, en ese sentido, la participación de un grupo multidisciplinario especializado en cada uno de los aspectos auditados mejoraría de manera muy significativa el proceso de auditoría.

Profundizar en cada una de las secciones y llevar a cabo la auditoría de manera sistemática con un grupo de trabajo, permitiría llegar a conclusiones más exactas y con un tiempo de respuesta mucho menor.

Un aspecto importante en lo que podría ampliarse el procedimiento es en los ambientes de red inalámbricos, dónde hoy existen grandes esfuerzos por parte de investigadores y de empresas privadas, que debido a la gran complejidad que representan los sistemas de información y a la gran cantidad de aspectos que deberían de analizarse este procedimiento sólo cubre una parte básica y el hecho de que cada día se agregan nuevas tecnologías se hace inevitable darle un carácter de periodicidad y actualización constante.

En un futuro también se podría considerar la auditoría forense, la cual busca identificar, preservar, analizar y presentar la evidencia electrónica de una intrusión de seguridad de tal manera que sea legalmente aceptable, mediante el uso de técnicas avanzadas de manipulación de datos en los equipos computacionales.

Referencias Bibliográficas

[AMADOR 01] **Seguridad Computacional**
Amador Donado, Soler, Niño Zambrano Miguel,
Publicación de la Universidad del Cauca Facultad de Ingeniería Electrónica y Comunicaciones. Programa de Ingeniería en Sistemas
2001

[ANONIMO,00] **Linux Máxima Seguridad**
Anónimo
Prentice Hall
2000

[ArCERT 00] **Manual de Seguridad en Redes**
Coordinación de Emergencia
en Redes Teleinformáticas de la
Administración Pública Argentina
Subsecretaría de Tecnologías Informáticas
2000

[CANO, 00] **Pautas y recomendaciones para elaborar Políticas de Seguridad Informática (PSI)**
Cano Martínez Jeimy J.
Red Iberoamericana de Criptografía y Seguridad de la Información
http://www.criptored.upm.es/guiateoria/gt_m142a.htm
Consultada Marzo 2005

[CANO, 04] **Apuntes sobre la inversión y gestión de la seguridad Informática**
Cano Martínez, Jeimy J.
Red Iberoamericana de Criptografía y Seguridad de la Información
http://www.criptored.upm.es/guiateoria/gt_m142q.htm
Consultada Agosto 2005

[Common,05-01] **Common Vulnerabilities and Exposures**
The standard for information Security Vulnerability Names
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0503
Consultada en Septiembre 2005

[Common,05-02] **Common Vulnerabilities and Exposures**
The standard for information Security Vulnerability Names
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0504
Consultada en Septiembre 2005

[Common,05-03] **Common Vulnerabilities and Exposures**
The standard for information Security Vulnerability Names
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0585
Consultada en Septiembre 2005

[Common,05-04] **Common Vulnerabilities and Exposures**
The standard for information Security Vulnerability Names
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-05035
Consultada en Septiembre 2005

[Common,05-05] **Common Vulnerabilities and Exposures**
The standard for information Security Vulnerability Names
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0923
Consultada en Septiembre 2005

[CORLETTI,04] **Matriz de Estado de Seguridad**
Corletti, Alejandro
Red Iberoamericana de Criptografía y Seguridad de la Información
http://www.criptored.upm.es/guiateoria/gt_m292d.htm
Consultada Agosto 2005

[CSI/FBI,04] **CSI/FBI Computer Crime and Security Survey**
CSI/FBI
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
Consultada Agosto 2005

[FORD, 01] **Tecnologías de interconectividad de redes.**
Merilee Ford, H Kim Lew
Pearson
2001

[HERNANDEZ, 00] **Auditoría en Informática**
Hernández Hernández, Enrique
CECSA
2000

[HispaSec, 05] **Hispasec. Seguridad y Tecnologías de Información**
http://www.hispasec.com/unaaldia/2540
Consultada Octubre 2005

[MACRO, 05-01] **Macromedia Support**
http://www.macromedia.com/support/coldfusion/ts/documents/tn17254.htm
Consultada Septiembre 2005

[MACRO, 05-02] **Macromedia Support**
http://download.allaire.com/publicdl/en/coldfusion/40/AllaireSecurityBulletin(ASB00-03)New4.0xCfcache.zip
Consultada Septiembre 2005

[McClure,02] **Hackers 3**
McClure Stuart, Scambray Joel, Kurtz George
McGrawHill
2002

[MICRO, 05-01] **Microsoft Support**
http://support.microsoft.com/kb/q152734/
Consultada Agosto 2005

[MICRO, 05-02] **Microsoft Support**
http://support.microsoft.com/kb/q154174/
Consultada Agosto 2005

[MICRO, 05-03] **Microsoft Support**
http://support.microsoft.com/support/kb/articles/Q165/0/05.ASP
Consultada Agosto 2005

[MICRO, 05-04] **Microsoft Support**
http://support.microsoft.com/kb/q282261/
Consultada Agosto 2005

[MICRO, 05-05] **Microsoft Support**
http://support.microsoft.com/kb/q179129/
Consultada Agosto 2005

[MICRO, 05-06] **Microsoft Support**
http://support.microsoft.com/kb/q143478/
Consultada Agosto 2005

[MICRO, 05-07] **Microsoft Support**
http://www.microsoft.com/technet/security/bulletin/ms99-020.mspx
Consultada Agosto 2005

[MICRO, 05-08] **Microsoft Support**
http://www.microsoft.com/technet/security/bulletin/MS03-039.asp
Consultada Agosto 2005

[MIGUEZ,03] **La Biblia del Hacker**
Míguez Pérez Carlos, Pérez Agudín Justo, Mariano-Matas Abel
Editorial Anaya Multimedia
2003

[MUÑOZ02] **Auditoría en Sistemas Computacionales**
Muñoz Razo, Carlos.
Pearson Educación
2002.

[NARANJO00] **Conceptos de la Auditoría de Sistemas**
Naranjo Siler, Ing. Alice
Facultad Filosofía-Especialidad Informática Guayaquil-Ecuador
http://www.impactalliance.org/ev.php?ID=4465_201&ID2=DO_TOPIC
Consultada en Agosto de 2004

[SECFCS,05-01] **Security Focus**
http://www.securityfocus.com/advisories/554
Consultada Agosto 2005

[SECFCS,05-02] **Security Focus**
http://www.securityfocus.com/bid/688
Consultada Septiembre de 2005

[SECFCS,05-03] **Security Focus**
http://online.securityfocus.com/infocus/1352
Consultada Septiembre de 2005

[SECFCS,05-04] **Security Focus**
http://www.securityfocus.com/bid/274
Consultada Septiembre de 2005

[SECSPC,05-01] **Security Space**
http://www.securityspace.com/es/smysecure/catid.html?id=10184
Consultada Septiembre de 2005

[QUINN,00] **La Auditoría informática dentro de las etapas de Análisis de Sistemas Administrativos**
Quinn, Eduardo Horacio

ANEXO A Software y Herramientas

- Lista de verificación para seguridad física.
- Lista de verificación para revisión de políticas de seguridad.
- Lista de verificación para plan de contingencia.
- *Software* para generación de palabras claves *Optimal Password Generator*
- *DicMake,* aplicación para generación de palabras claves.
- *John The Ripper* aplicación para llevar a cabo ataques por fuerza bruta
- *Goldeneye* para ataques de fuerza bruta
- Software de escaneo de vulnerabilidades *LanGuard*.
- Software de escaneo de vulnerabilidades *Dragonsfot Secure Scanner*
- Software de escaneo de vulnerabilidades *Shadow Security Scanner*
- *Ethereal.* Sniffer para obtención de información crítica y analizador de red..

ANEXO B Glosario de Términos

- **A** -

Access Point. (Punto de acceso) Dispositivo que permite unir los diferentes elementos de una red inalámbrica con la red cableada tradicional

ACL. (Listas de control de acceso) permite definir los derechos de acceso a los archivos a los usuarios del sistema.

- **B** -

Backbone. Una línea de alta velocidad o serie de conexiones que conforman el principal flujo de información contenida en una red.

BGP. (*Border Gateway Protocol*) Protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP.

- **C** –

CGI. (*Common Gateway Interface*) Conjunto de reglas que describen cómo un servidor Web se comunica con una pieza de software en la misma máquina, y como la otra pieza de *software* (el programa "CGI") habla con el servidor web.

Cracker. (*crack*, romper) Persona que diseña programas *cracks* informáticos para modificar el comportamiento de un software.

- **D** -

DMZ. Zona desmilitarizada. Área de una red de computadoras que está entre la red de computadoras interior de una organización y una red de computadoras exterior, generalmente la Internet. La zona desmilitarizada permite que servidores interiores provean la red exterior de servicios, mientras protege la red interior de intromisiones.

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

DoS. (Denial of Services) Denegación de servicios. Bloqueo o paralización de un servicio para que no pueda ser utilizado por sus usuarios. Acción iniciada por una persona o por cualquier otra causa, que incapacite al hardware, software o ambos, de un host y que lleve a que no se pueda llegar a su sistema.

- **E** –

Exploits. (to exploit - aprovechar) código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios.

- **F** -

Firewall. Sistema de defensa basado en un conjunto de medidas ya sea de hardware o de software que funciona como barrera defensiva entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local e Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

- **G** -

Gateway. Equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation)

- **H** –

Hacking. Acceso no permitido a un sistema informático

Host. Computadora conectada a una red. Nodo con nombre de dominio.

- **I** -

IDF. Intermediate Distribution Facilities. Unidad para distribución intermedia.

IDS. Mecanismos para la detección de intrusos. Detecta paquetes y datos que no deben circular por la red. Se clasifican por su ámbito de vigilancia en HIDS (Host Intrusión Detection System), NIDS (Network Intrusión Detection System), y DIDS (Distributed Intrusión Detection System)

ICMP. El Protocolo de Control de Mensajes de Internet es uno de los protocolos centrales de la suite de protocolos de Internet. Es usado principalmente por los Sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible ó que un router ó host no puede ser localizado

Internet. Es un vasto conjunto de redes interconectadas que utilizan la familia de protocolos TCP/IP

Intranet. Es una red privada dentro de una compañía u organización que utiliza el mismo tipo de software usado en el Internet público, pero que es sólo para uso interno

IP. (Internet Protocol) Protocolo de Internet. Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados

Ipsec. (Internet Protocol security) es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y cifrado y, de esta manera, asegurar las comunicaciones a través de dicho protocolo.

- **M** -

MDF. Main Distribution Facility. Unidad para Distribución Principal.

- **N** -

NAT. (Network Address Translation)Traducción de direcciones de red.

NetBIOS. (Network Basic Input/Output System) Protocolo de aplicación para compartir recursos en red, engloba un conjunto de protocolos de nivel de sesión, que proveen 3 tipos de servicios: servicio de nombres, servicio de paquetes servicio de sesión.

- **O** -

OSPF. (Open Shortest Path First) Protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado idéntica en todos los ruteadores de la zona.

- **P** -

POP. (Point of Presence) Punto de la red donde se conectan los dispositivos de comunicación. Donde un Proveedor de Servicios Internet ofrece acceso a la red Internet

Proxy. Programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual de esa representación es la de permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Puerto. Conexión bien sea física o lógica para el envío y recepción de datos. Existen servicios de red asociados específicamente a un número de puerto.

- **R** –

Router. Dispositivo que maneja la conexión entre dos o más redes. Los ruteadores se encargan de buscar la dirección de destino de los paquetes que pasan por ellos y deciden hacia cual ruta enviarlos.

RPC Services. (Remote Procedure Call) Servicios para las llamadas a procedimientos remotos. Permite ejecutar comandos en un cliente para su ejecución en un servidor remoto.

- **S** -

Scanner. Dispositivo de software que comprueba una red buscando posibles vulnerabilidades de seguridad mediante el análisis de toda la red en busca de actualizaciones de seguridad que falten, service packs, recursos compartidos abiertos, puertos abiertos, cuentas de usuario que no se utilizan, etc.

Sript. Conjunto de instrucciones ejecutadas mediante un interprete (*parse*r) independiente del hardware y sistema operativo de un sistema.

Service Pack. Paquete de actualizaciones que contiene archivos en sus versiones más recientes que solucionan problemas previamente conocidos

Servidor. Una computadora que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, servicios de aplicaciones,

SSL. (Secure Socket Layer). Es un protocolo diseñado por la empresa Netscape Communications, que permite cifrar la conexión, incluso garantiza la autenticación. Se basa en la criptografía asimétrica y en el concepto de los certificados. La versión estandarizada por el IETF se conoce como TLS.

SSH. **(**Secure SHell). Este protocolo sirve para acceder a máquinas remotas a través de una red, de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Sniffing. Técnica implementada normalmente en una aplicación para la captura de paquetes de red, permite monitorear y analizar el tráfico de una red, generalmente utilizado con fines maliciosos.

Spoofing. Es una técnica para crear tramas TCP/IP que utilicen una dirección IP falsa; la idea de este ataque es la siguiente: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

- **T** -

TCP. (Transmission Control Protocol) Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

- **U** -

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

- **V** -

VPN. Virtual Private Network (Red Privada Virtual) es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.