UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO.

FACULTAD DE CONTADURÍA DE CIENCIAS ADMINISTRATIVAS.

“DIAGNOSTICO A LA SEGURIDAD EN REDES DEL COBAEM”.

TESINA

PARA OBTENER EL TITULO DE:
LICENCIADA INFORMÁTICA ADMINISTRATIVA.

PRESENTA:
BLANCA ODILIA ROBLERO MORALES.

ASESORA:
DR.MA. HILDA RODALES TRUJILLO.

Morelia, Mich. Abril del 2013

Agradecimiento

A DIOS:

Por darme fortaleza y serenidad en los momentos difíciles, salud y su total compañía en A cada instante de mi existencia. A dios por darme vida para poder realizar mis estudios.

A MIS PADRES EDILSAR Y CARALAMPIA:

Con infinita gratitud A mis padres Edilzar Roblero y Caralampia Morales, porque sin ellos yo nada seria, agradezco su apoyo y las palabras de aliento en todo momento, y a quienes debo todo lo que soy y seré en esta vida, y ser los padres más hermosos en la inspiración para lograr mi meta y por darme su total confianza. Gracias papas por su gran amor incondicionalmente, son los mejores paredes los amo.

A MIS HERMANOS ALBERT, TRINY, CLARIBEL Y KARLA:

A mis hermanos (as), por estar siempre brindándome su apoyo y cariño incondicional. Por ser un faro que siempre estuvo.

A MI ABUELITA ODILIA:

A mi abuelita hermosa que amo, por ser el ángel que siempre estuvo brindándome su cariño y buenos deseos para lograr mi meta.

A MI TIO MIGUEL Y SU ESPOSA:

A mi tío que siempre estuvo apoyándome en todo y gracias por sus consejos. Y su esposa por su bridarme su apoyo incondicionalmente.

A MIS PRIMOS ROBER, MARITZA, CESAR, DANIELA, IVAN:

A mis primos que siempre me apoyaron con moralmente.

A MI ASESORA DE TESINA MA. HILDA RODALES TRUJILLO:

A mi asesora por brindarme toda su paciencia, comprensión, apoyo y firmeza incondicionalmente en la realización de la tesina.

A MIS PROFESORES:
Con profundo respeto y admiración a mis maestros, que con gran paciencia y vocación dieron siempre lo mejor de ellos, no solo como maestros si no como guías y ejemplos a seguir en la vida profesional.

A MIS AMIGAS YESSY, ANA, FLORY, DANNY, CIELO, MARIA, ERE, TERE, VANE, JULIA, LESVI, SIRIA:
Por ser la personas que no dejaron de aconsejarme de no cambiar y luchar por mi carrera. Pedirle a dios por mí y darme su cariño.

A MIS AMIGO PEDRO, GERMAN, MARIO:
Por ser las persona que no dejaron de aconsejarme durante mi carrera. Y por darme su cariño.

A MI U.M.S.N.H.
Por haberme formado académicamente y por permitir mí desarrollo profesional.

LIC. VERERO:
Gracias ella por darme la oportunidad a ver realizado la investigación de tesina.

COBAEM:
Gracias COBAEM por la información para realzar o llevar acabo mi tesina.

A MIS FAMILIARES Y AMISTADES:
Gracias por darme sus consejos y por darme su cariño.

Muchas gracias a todos

Introducción

En la vida siempre ha existido la evaluación, donde ella ha servido y debe servir para mejorar el nivel de vida de la humanidad, tanto espiritual, tecnológica, en las comunicaciones, etc. Todo esto se resumen a lo que es la información, y esta puede ser pública o privada.

En este trabajo se busca para conocer acerca del diagnóstico a la seguridad en redes y también para darnos una idea en el instituto de **COBAEM** así mismo los usuarios este consientes de la configuración de las redes para cada equipo y si darle una buena utilización a los equipos, obtener eficiencia y eficaz para los usuarios así tener a tiempo sus trabajos correspondientes.

En el primer capítulo, hablamos ampliamente de Las generalidades de redes información, el concepto informática, redes para conocer un poco y comenzamos por definir, los tipos de redes así podemos encontrar una diversidad de concepto la seguridad de información los principios de seguridad informáticos, tipos de seguridad, amenazas de seguridad informática, análisis de riesgo, y el procesos del análisis de riesgo elementos de estudios, es de vital importancia.

En el segundo capítulo hablamos de auditoria y concepto de auditoria informática, tipos y clases de auditoría, auditoria informática de sistemas, auditoria información de redes, auditoria de la seguridad informática, informes de auditoría y tipos de dictamen, así también el modelo ISO, estándares de calidad, estándares de sistemas de gestión, metodología para desarrollo de auditoria en informática, planeación de auditoria e informática, se realizó una encuesta.

Finalmente en el tercer capítulo desarrollamos el caso práctico, se muestra el análisis de la información recabada a proponer elementos de seguridad en redes, ya que es la base de donde partimos para el desarrollo de esta tesina, en primera instancia definimos los antecedentes que tiene, en segunda instancia precisamos en su giro, estructura de organización, función del sistema de COBAEM, aplicación a la mejora de la metodología de la auditoria en redes en donde mencionamos cada función aplicada con los pasos de la metodología para obtener una auditoria.

Sin más que agregar comenzamos con el desarrollo del trabajo esperando que sea de mucha utilidad la presente investigación y el diagnostico al desarrollado, para conocer un poco más lo que el futuro redes nos tiene preparado.

Problemática

En la entrevista con el encargado del área de redes el Ing. Francisco Daniel Díaz Villagómez manifestó tener que la problemática más frecuentes era con la seguridad del sistema relacionada con el resguardo de la información, robo, las amenazas de virus. Lo cual hace deficiente su función como administrador de la red de información en el instituto.

Así mismo manifiesto su interés por el grado de inseguridad que se guarde.

Objetivo general

- Diagnosticar la seguridad en redes del instituto del COLEGIO DE BACHILLERES DEL ESTADO DE MICHOACAN.

Objetivo especifico

- Análisis del funcionamiento de la red
- Investigar las metodologías existente para emitir un diagnostico en la seguridad de redes.
- Investigar los tipos de diagnóstico en la auditoria informática.

Justificación

Como la inseguridad se da en muchas maneras en nuestro entorno social, en las redes no es la excepción. Las organizaciones, empresas, universidades, etc. Buscan tener la mayor seguridad en sus esquemas, para no tener pérdidas en su economía, de su privacidad y de su confidencialidad.

Para poder prevenir la seguridad de la red es una característica prominente de la red asegurando responsabilidad, confidencialidad, integridad esto se puede hacer simplemente si tener constantemente actualizando los antivirus firewalls y tener respalda toda la información en un lugar de seguridad.

La seguridad en redes es indispensable para facilitar la eficiencia y tener una mejor utilización en los diferentes equipos del instituto de **COBAEM** y así los usuarios leden un mejor cuidado los equipos. Que cada usuario lleva su diferente información de los planteles, del estado de Michoacán.

Debemos conocer la inseguridad en la redes de información son las amenazas externas e internas tales como problemas basados en email de la seguridad de red ,virus ,spam, los gusanos ,los troyanos y intentos de ataques de seguridad, robo de información etc. La información sobre los diversos tipos de prevención debe de estar actualizados de acuerdo para garantizar su funcionamiento.

Esta aplicación es con la finalidad de tener un mejor control con todos los equipos y así mismo uno poder habilitar o deshabilitar cualquier acceso que el usuario requiera en el momento que lo necesite para realizarsus actividades durante el día.

Capítulo I Generalidades de redes de información

Informática

La informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales.

La informática abarca también los principales fundamentos de las ciencias de la computación, como la programación para el desarrollo de software, la arquitectura de las computadoras y del hardware, las redes como internet y la inteligencia artificial.

Redes

Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Las redes permiten la conexión entre varios ordenadores o periféricos. Cuando están en proximidad geográfica se llaman redes locales y cuando conectan ordenadores distantes se denominan redes de telecomunicación.(Suarez, 2007)

Una red es un conjunto de dispositivos (a menudo denominado nodos) conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. Los enlaces conectados con los dispositivos se denominan a menudo canales de comunicación.(FOROUZAN, 2002)

1.1 Tipos de redes

Red de área local (LAN, local área network) suele ser una red de propiedad privada que conecta enlaces de una única oficina, edificio o campus. Dependiendo de las necesidades de la organización donde se instale y el tipo de tecnología utilizada, una LAN puede ser tan sencilla como dos pc y una impresora situados en la oficina de la casa.

Redes de área metropolitana (MAN, metropolitan área network) ha sido diseñada para que se pueda extender a lo largo de una ciudad entera. Puede ser una red única, como una red de televisión por cable, o puede ser una forma de conectar un cierto número de LAN a LAN y de dispositivo a dispositivo.

Red de área amplia (WAN, wide área network) proporciona un medio de transmisión a larga distancia de datos, voz, imágenes e información de video sobre grandes áreas geográficas que pueden extenderse a un país, un continente o incluso el mundo entero.

Topologías de red

Redes en Malla: cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dispositivos que conecta. Todos los nodos se comunican directamente entre sí.

Redes en estrella: cada dispositivo solamente tiene un enlace punto a punto dedicado con el control, habitualmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí. Es un nodo central que normalmente es un hub y el están conectados todos los pc, la información pasa por el hub para luego ir a su destino.

Redes en árbol: es una variante de la estrella. Como en la estrella, los nodos del árbol están conectados a un concentrado central que controla el tráfico de la red. Tiene un nodo troncal que suele ser un hub desde el que se ramifican los demás nodos.

Redes en bus: es multipunto. Un cable largo actúa como red troncal que conecta todos los dispositivos en la red. Los nodos se conectan al bus mediante cables de conexión (latiguillos) y sondas. Un cable de conexión es una que va desde el dispositivo al cable principal. Todas las máquinas están conectadas a un único cable por donde pasa toda la información.

Redes en anillo: cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino.: Es un anillo cerrado donde cada nodo o PC está conectado con sus nodos adyacentes formando un anillo. La información se transmite de nodo en nodo. (Stallings, 2000).

1.2 La seguridad de la información

La definición de y el objetivo de la seguridad en redes es mantener la integridad, disponibilidad, privacidad sus aspectos fundamentales control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permita el control de lo adecuado.

La seguridad informática es la disciplina que ocupa de diseñar las normas procedimientos, métodos y técnicas destinadas a conseguir un sistema de información suegro y confiable.

La seguridad física: Son tareas y mecanismos cuyo objetivo es proteger al sistema y, por tanto indirectamente a la información de peligros físicos y lógicos. Se refiere a la protección del hardware y de los soportes de datos.

- ✓ Equipamiento: es necesario proteger los equipos de cómputo en áreas en las cuales el acceso a lo mismo solo sea para el personal autorizado.
- ✓ Incendios: los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.
- ✓ Respaldo de datos: guardar copias de seguridad de la información del sistema en lugar seguro.
- ✓ Dispositivos físicos: de protección, como pararrayos, detectores de humo y extintores, cortafuegos por hardware, alarmas contra intrusos, sistemas de almacenamiento interrumpida (para picos y cortes de corrientes eléctrica) o mecanismo de protección contra instalación.
- ✓ Cableado: los cables que se utilizan para construir las redes locales, van desde el cable normal al cable coaxial o la fibra óptica.

La seguridad lógica: Los mecanismos y herramienta de seguridad lógica tienen objetivo proteger digitalmente la información de manera directa. Se refiere a la seguridad del uso del software a la protección de los datos, procesos y programas.

- ✓ Control de acceso: estos pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos mediante nombres de usuarios, contraseñas en un paquete específico de seguridad o en cualquier otro utilitario.
- ✓ Roles: el acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.
- ✓ Cifrado de datos encriptación: los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Emisor y receptor son conocedores de la clave y a la llegada del mensaje se produce el descifrado. El cifrado de datos fortalece la confidencialidad.
- ✓ Transacciones: también pueden implementarse controles a través de las transacciones.
- ✓ Limitación a los servicios: estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

- ✓ Antivirus: detectan e impiden la entrada de virus y otro software malicioso, en caso de infección tiene capacidad de eliminar y de corregir los daños que ocasionan en el sistema.(Aguilera, 2010)

1.3 Principios de Seguridad Informática

Confidencialidad: consiste en proteger la información contra la lectura no autorizada explícitamente.
La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos de los datos.

Integridad: es necesario proteger la información contra la modificación sin el permiso del dueño.
Significa que se debe asegurar que la información no ha sido alterada por medios no autorizados o desconocidos. Un atacante no debe ser capaz de sustituir información legítima por falsa.

Autenticidad: en cuanto a telecomunicaciones se refiere, la autenticación garantiza que quien dice ser es realmente.

Debe ser posible para un usuario establecer el origen de la información. Un atacante no debe tener la capacidad de hacerse pasar por otro usuario.

Posesión: es mantener, controlar y tener la habilidad de usar la información. La posesión es la habilidad de realmente poseer y controlar la información y como es usada.

No repudio: ni el origen ni el destino en un mensaje deben poder negar la transmisión.

Disponibilidad de los recursos y de la información: nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella.
Significa que todos aquellos elementos que sirven para el procedimiento de la información, así como los que sirven para facilitar la seguridad, este activo y sean alcanzables siempre que se requiera.

Consistencia: se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

Control de acceso a los recursos: consiste en controlar quien utiliza el sistema o cualquiera de los recursos que ofrece y como lo hace.

Utilidad: utilidad de la información para un propósito. El valor de la información recae en su utilidad.

Auditoria: consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, que es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.(Yumar, 2008)

1.4 Tipos de seguridad

Activa: Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

Pasiva: Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema.(Aguilera, 2010)

1.5 Amenazas a la seguridad de la información

Se entiende por amenaza a la seguridad de la información, una condición del entorno del sistema de información que dada una oportunidad, podría producir una violación de seguridad (confidencialidad, integridad, disponibilidad).
Según Marcano (2003), las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información.

González (2003), selecciona las amenazas en las siguientes categorías:

a) Interrupción: un recurso del sistema es destruido o se vuelve no disponible, este ataque es contra la disponibilidad.
b) Intercepción: una entidad no autorizada consigue acceso a un recurso, este es contra la confidencialidad.
c) Modificación: una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo.
d) Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema.(Bello, 2005)

1.6 Análisis de riesgos

La seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema (Aguilera, 2010)

Riesgos

Se denominar riesgo a la posibilidad de que se materialice o no amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.
Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- ✓ Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
- ✓ Aplicar medios para disminuirlo o anularlo.
- ✓ Transferirlo (por ejemplo, contratando un seguro).

1.6.1 Elementos de estudio

Para comenzar a analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta los siguientes elementos: activos, amenazas, riesgos, vulnerabilidades, ataques e impactos.

Activos
Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos.

Podemos clasificarlos en los siguientes tipos:

Datos. Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están en servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo.

Cada tipo de dato merece un estudio independiente de riesgo por la repercusión que su deterioro.

Software. Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tengan establecido.

Hardware. Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información.

Redes. Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancias.

Soportes. Los lugares en donde la información queda registrada y almacenada durante largos periodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).

Instalaciones. Son los lugares que albergan los sistemas de información y de comunicaciones.

Personal. El conjunto de personas que interactúan con el sistema de información, administradores, programadores, usuarios internos y externos y resto de personal de la empresa.

Amenazas

Dentro del campo de la auditoria informática existen riesgos, amenazas y vulnerabilidades que son diferentes.

La amenaza se define como la causa potencial de un índice no deseado, que causa daño a un sistema o a la organización.

En sistemas de información se entiende por amenaza la presencia de unos o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortos electrónicos, fallos de hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software virus, troyanos, gusanos o el robo, destrucción o modificación de la información.

En función de tipo de alteración, daño o intervención que podría producir sobre la información, las amenazas se clasifican en cuatro grupos:

De interrupción. El objetivo de la amenaza es deshabilitar el acceso a la información.

De interceptación. Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

De modificación. Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificaran.
De fabricante. Agregar información falsa en el conjunto de información del sistema.

Vulnerabilidades
Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas.

Ataques
Se dice que se ha producido un ataque accidental o debilidad contra el sistema cuando se ha materializado una amenaza.

Impactos
Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser cuantitativos, si los perjuicios pueden cuantificarse económicamente, o cualitativos, si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

1.6.2 proceso del análisis de riesgo

Para implantar una política de seguridad en un sistema de información es necesario seguir un esquema lógico.

- Hacer inventario y valoración de los activos.
- Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.
- Identificar y evaluar las medidas de seguridad existentes.
- Identificar y valorar las vulnerabilidades de los activos a las amenazas que les afectan.
- Identificar los objetivos de seguridad de la organización.
- Determinar sistemas de medición de riesgos.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección.(Aguilera, 2010).

Capitulo II Auditoria

La auditoría es una función de dirección cuta finalidad es analizar y apreciar, con vistas a las eventuales las acciones correctivas el control interno de las organizaciones para garantizar la integridad de su patrimonio la velocidad de su información y el mantenimiento de la eficiencia de su sistema de gestión.

Auditoria interna: es realizada con medios y recursos propios de la organización, por un departamento propio de la empresa en el caso de que se haya creado y cumpla con todos los requisitos necesarios para realizar de forma clara sus funciones. Este equipo deberá estar formado por expertos en la materia y deberán dar cuenta ante el responsable.

Auditoria externa: es realizar con medios y recursos ajenos normalmente remunerada con un servicio contratado, participa un profesional de este campo de forma independiente y con una experiencia y un perfil contrastado para poder realizar esa función.(Echenique, Auditoria Informatica, 2001)

2.1 Auditoria informática

La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar su tarea.

Es un conjunto de procedimientos y técnicas para evaluar y controlar parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática.

Los procedimientos de auditoria con informática varían de acuerdo con la filosofía y técnica de cada organización y departamento de auditoria en particular. Sin embargo, existen ciertas técnicas y / o procedimientos que son compatibles en la mayoría de los ambientes de información. Estas técnicas caen en dos categorías: métodos manuales y métodos asistidos por computadora.(Echenique, Auditoria en Informatica, 2003)

2.1.1Tipos y clases de auditoria

El control del funcionamiento del departamento de informática con el exterior, con el usuario se realiza por medio de la dirección.

Auditoría Informática de Explotación:

La Explotación Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fábrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la explotación informática se dispone de una materia prima, los datos, que sea necesario transformar, y que se sometan previamente a controles de integridad y calidad.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones:

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Preprogramacion y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario.(Echenique, Auditoria Informatica, 2001)

2.1.2 Auditoria informática de sistemas

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas.La importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos: Engloba los Subsistemas de Teleproceso, Entrada/Salída, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera.

Tunning: Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal de Técnica de Sistemas.

El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- Cuando existe sospecha de deterioro del comportamiento parcial o general del Sistema
- De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.(Piattini, 2001).

2.1.3 Auditoria de redes

La infraestructura las tecnologías de información y de las comunicaciones (TIC) se ha convertido en un activo empresarial estratégico y la red constituye su núcleo. La auditoría de redes es una serie de mecanismos mediantes los cuales se pone a prueba una red

informática, evaluando el desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información. Consiste en identificar:

- Estructura física (hardware, topología)
- Estructura lógica (software, aplicaciones)

La identificación se lleva a cabo en los equipos, la red, el internet y extranet. Las etapas de la auditoria de redes son:

- Análisis de la vulnerabilidad
- Estrategias de saneamiento
- Plan de contención ante posibles incidentes
- Seguimiento continuo del desempeño del sistema

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte.

Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad.La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

Los términos más usados en una red de comunicaciones.

ROUTER. Las direcciones que se escriben y las identifica, este a su vez pone los paquetes en otra red si es necesario. El Router es el que se encarga de organizar y controlar el tráfico.

DNS. Esto lo que hace es que identifica y busca los nombres de los dominios. Se utilizan para buscar principalmente las direcciones IP.

PROXY. Es usado como intermediario; en muchas empresas lo utilizan como manera de seguridad. Este también tiene la función de establecer y compartir con todo los usuarios una única conexión de internet. El proxy abre la dirección web o URL, este aprueba o desaprueba los paquetes para luego enviarlos a internet.

FIREWALL. Tiene dos propósitos fundamentales: prevenir intromisiones indeseables provenientes del internet y evitar que la información de importancia que existe en nuestra computadora sea enviada al internet.

HUB. Se utiliza para conectar distintos tipos de cable o redes de área local. Para los que no lo saben, el término “hub” concentrador. Es el núcleo o centro de conexión de una red.

IP. Es un tipo de protocolo que empaqueta y etiqueta los paquetes cargados con datos y los pone en camino.

ROUTER SWITCH. Es tal vez mucho más eficiente que el Router y más rápido. Este suelta los paquetes enlutándoles por su camino.

TCP. Es un estándar de comunicación muy extendido y de uso muy frecuente para software de redes. El TCP es un tipo de protocolo de internet.

Puertos de comunicación. Son herramientas que permite manejar e intercambiar datos entre una computadora.

Protocolos. Son las distintas maneras que existen de comunicaciones; existen distintos tipos de protocolos cada uno diseñado para una función y actividad específica.(Piattini, 2001)

2.1.4 Auditoria de la seguridad información

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.(Piattini, 2001)

2.2 Informe de auditoría y tipos de dictamen

En todos los casos en que el auditor realiza una revisión, debe expresar una opinión. La opinión, diagnostico o dictamen es la expresión emitida acerca del resultado del proceso de auditoría.

Dictamen favorable o limpio

La opinión calificada como favorable, sin salvedades o limpia debe manifestarse de forma clara y precisa, es el resultado de un trabajo realizado sin limitaciones de alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.

Salvedad

Al respecto de las salvedades cuando sean significativas en relación con los objetivos de auditoria y con precisión la naturaleza y razones, se realiza según las circunstancias.

- Limitaciones al alcance del trabajo realizado, restricciones por parte del auditado.
- Incertidumbre cuyo resultado no permita una previsión razonable.
- Irregularidades significativas.
- No hay suficiente evidencia comprobatoria

El acceso a los activos solo debe permitirse de acuerdo con autorizaciones de la administración.

Evaluación de la eficiencia de las salvaguardas existentes en la relación al riesgo que afrontan.

Abstención de opinión

Establece que el auditor no expresa una opinión normalmente por los siguientes:

- Incertidumbres significativas de un modo tal que impida al auditar formarse una opinión.
- Irregularidades.
- Limitaciones en el alcance de la auditoria.
- La existencia de incertidumbre cuando su importancia es significativa

Corrección

Utilizamos la corrección de los métodos de salvaguardar de los activos para verificar la existencia de estos activos.
Y que los métodos para salvaguardar los activos de diferentes tipos de riesgos tales como robo, incendios, actividades impropias o ilegales, así como de elementos naturales como son los terremotos, inundaciones, etcétera.
Los auditores deberán evaluar si el empleo de los recursos se realiza en forma económica y eficiente.
La administración es responsable de establecer estándares de operación para medir la eficiencia y economía en el uso de los recursos.(Piattini, 2001)

2.3 El modelo ISO

Un modelo de referencia que fue definido por la ISO (International Standards Organization) como un estándar para las comunicaciones mundiales. Define una estructura para la implementación de protocolos en siete estratos o capas.El modelo de red descriptivo creado por ISO

Es un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

Una de las necesidades más acuciantes de un sistema de comunicación es los establecimientos de estándares, sin ellos solo podrán comunicarse entre sí equipos del mismo fabricante y que usaran la misma tecnología.

La conexión entre equipos electrónicos se ha ido estandarizando paulatinamente siendo las redes.

Otros organismos internacionales que generan nomas relativas a las telecomunicaciones son: ITU-TSS (antes CCITT), ANSI, IEEE e ISO.

La ISO (internacional organizaciónforo standarisation) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudara a comprender mejor el funcionamiento de las redes de ordenadores.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI describe siete niveles para facilitar los interfaces de conexión entre sistemas abiertos.

1. Físico. Se ocupa de la transformación del flujo de bits a través del medio.
2. Enlace. Divide el flujo de bits en unidades con formato tramas intercambiando estas unidades mediante el empleo de protocolos.
3. Red. Establece las comunicaciones y determina el camino que tomaran los datos en la red.
4. Transporte. La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha requerido enviar el emisor, y a veces asegurar al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.
5. Sesión. Establecer la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez.
6. Presentación. Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros son características diferentes.
7. Aplicación. Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones específicas en la red. (FOROUZAN, 2002)

2.4 Estándares de calidad

Es un proceso que parte de los criterios de autoevaluación de una organización. Estos sirven para medir la excelencia del servicio prestado por organización. El principal objetivo es crear aprendizaje continuos en la gestión de las organizaciones promoviendo así que dichas organizaciones puedan rendir al máximo según los objetivos planteados, y ofrecer a personas usuarias producto o servicio de la más alta calidad.

En estos casos es donde se diseñan estándares y normas por medio de los cuales se busca apreciar los cumplimientos en cuanto a la calidad esperada en relación con la calidad realmente alcanzada; éstos pueden ser muchos tipos de estándares de medición y muy variados aspectos. (Muñoz, 2002)

- Grupo de trabajo en protocolos LAN de capas superior 802.1: generalidades y arquitectura, interconexión con puentes, LAN puenteadas virtualmente.
- Grupo de trabajo en control de enlace lógico 802.2: inactivo
- Grupo de trabajo en Ethernet 802.3: método de acceso y señalización física.

- Grupo de trabajo en redes en bus con paso de testigo (token bus) 802.4: métodos de acceso y señalización física (inactivo).
- Grupo de trabajo en redes en anillo con paso de testigo (token ring) 802.5: métodos de acceso y señalización física.
- Grupo de trabajo en redes de área metropolitana 802.6: método de acceso y señalización física (inactivo).
- TAG de banda ancha 802.7: grupo de asesor en tecnología de banda ancha (inactivo).
- TAG de fibra óptica 802.8: grupo de asesor en la tecnología de fibra óptica.
- Grupo de trabajo en LAN isócronas 802.9: método de acceso y señalización física.
- Grupo de trabajo en seguridad 802.10: diversos niveles de seguridad para todos los estándares IEEE 802.
- Grupo de trabajo en LAN inalámbricas 802.11: método de acceso y señalización física.
- Grupo de trabajo en demanda de prioridad 802.12: método de acceso y señalización física.
- 802.13: no usado
- Grupo de trabajo en cable modem 802.14.
- Grupo de trabajo en redes inalámbricas de área personal 802.15: estándares para redes inalámbricas para cubrir distancias cortas.
- Grupo de trabajo de acceso inalámbrico de banda ancha 802.16.
- Grupo de estudio QoS/control de flujo.
- El IEEE 802 ha desarrollado una serie de estándares. En cada estándar se especifica la técnica de acceso al medio (MAN, médium Access control), además de diversas opciones de medios de transmisión con distintas velocidades.
- El protocolo LAN 802 más utilizado es el 802.3, basado en las especificaciones iniciales de Ethernet.
- Una aproximación potente y flexible es la utilizada en las LAN ATM. Este tipo de LAN generaliza la tecnología y protocolos ATM, desarrollados para entornos de área amplia, al contexto de las redes corporativas.
- El IEEE 802 ha desarrollado además un estándar para LAN inalámbricas, utilizado tecnologías de infrarrojos y de espectro expandido.
- IEEE 802. Estándar que especifica la relación de los estándares IEEE y su interacción con los modelos OSI de la ISO, así como las cuestiones de interconectividad y administración de redes.
- IEEE 802.2. Control lógico de enlace (LLC), que ofrece servicios de "conexión lógica" a nivel de capa 2.
- IEEE 802.3. El comité de la IEEE 802. 3 definió un estándar el cual incluye el formato del paquete de datos para Ethernet, el cableado a usar y el máximo de distancia alcanzable para este tipo de redes. Describe una LAN usando una topología de bus, con un método de acceso al medio llamado CSMA/CD y un

cableado coaxial de banda base de 50 ohms capaz de manejar datos a una velocidad de 10 Mbs.

- IEEE 802.3 10Base5. El estándar para bus IEEE 802.3 originalmente fue desarrollado para cable coaxial de banda base tipo Thick como una norma para Ethernet, especificación a la cual se hace referencia como 10Base5 y describe un bus de red de compuesto por un cable coaxial de banda base de tipo thick el cual puede transmitir datos a una velocidad de 10Mbs. sobre un máximo de 500 mts.
- IEEE 802.3 10Base2. Este estándar describe un bus de red el cual puede transmitir datos a una velocidad de 10 Mbs sobre un cable coaxial de banda base del tipo Thin en una distancia máxima de 200 mts.
- IEEE 802.3 STARLAN.El comité IEEE 802 desarrollo este estándar para una red con protocolo CSMA el cual hace uso de una topología de estrella agrupada en la cual las estrellas se enlazan con otra. También se le conoce con la especificación 10Base5 y describe una red la cual puede transmitir datos a una velocidad de 1 Mbs hasta una distancia de 500 mts. Usando un cableado de dos pares trenzados calibres 24.
- IEEE 802.3 10BaseT. Este estándar describe un bus lógico 802.3 CSMA/CD sobre un cableado de 4 pares trenzados el cual está configurado físicamente como una estrella distribuida, capaz de transmitir datos a 10 Mbs en un máximo de distancia de 100 mts.(FOROUZAN, 2002)

2.4.1 Estándares de sistemas de gestión

Esta norma internacional especifica los requisitos de un sistema de gestión de la calidad. La edición actual, ISO 9001:2008, sustituye a la tercera edición (ISO 9001:2000) que ha sido modificada para clarificar puntos en el texto y aumentar la compatibilidad con otras normas.

ISO 9001:2008, en su apartado compatibilidad con otros sistemas de gestión, hace referencia a la integración con otros sistemas de gestión. Esta norma internacional no incluye requisitos específicos de otros sistemas de gestión, tales como aquellos particulares para la gestión ambiental, gestión de la seguridad y salud ocupacional, gestión financiera o gestión de riesgos.

2.5 Metodologías para desarrollo de auditoria en informática

Dice el autor plattini (2001), en esta metodología es una secuencia de pasos lógica y ordenada de preceder para llegar a un resultado. Generalmente existen diversas formas de obtener un resultado determinado, y de estos se deriva la existencia de varias metodologías para llevar a cabo una auditoria informática.

1. Planeación

Esta consiste en la elaboración de los programas de trabajo que se llevan a cabo durante la revisión a la entidad auditada.

2. Trabajos preliminares

Consiste básicamente, de una serie de entrevistas con nuestros clientes, las cuales tienen como objetivo dejar en claro las características básicas del trabajo que se va a realizar, que es lo que quiere el cliente y que hará, en términos generales, el auditor.

3. Diagnostico administrativo

El diagnostico administrativo tiene por objetivo, proporcionarnos una panorámica de cómo la empresa percibe y practica la administración.

4. Investigación previa

Aquí conoceremos la empresa y de ser posible validaremos la problemática que nos fue expuesta por el cliente. Después de esta fase se estará en posibilidades de hacer una mejor estimación del tiempo.

5. Elaboración del programa de la auditoria informática

Todo buen administrador debe planear sus actividades y el auditor no debe ser la excepción, el programa señala las actividades que han de realizarse, fechas de inicio y termino, así como los tiempos.

6. Obtención de información

En esta fase se obtendrá toda la información pertinente sobre el caso estudiado, pudiendo recurrir a herramientas como entrevistas, encuestas, observación, etc. Dependiendo el tipo de información que necesite.

7. Análisis, clasificación y evaluación de la información

Análisis y clasificación de la información podrá realizarse por métodos estadísticos.

Evaluación es aquí en donde se pone a prueba el talento del auditor, porque para entender e interpretar la información y continuar con el siguiente pasó.

8. Alcance y Objetivos de la Auditoría Informática.

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

9. Estudio inicial del entorno auditable.

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.

10. Determinación de los recursos necesarios para realizar la auditoría.

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

11. Elaboración del plan y de los Programas de Trabajo.

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo.

12. Actividades propiamente dichas de la auditoría.

La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

13. Confección y redacción del Informe Final.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.(Piattini, 2001)

2.6 Planeación de auditoria e informática

Proceso de planeación en informática

Esto se hizo con la función de la informática esa en tiempos a corto, mediano y largo plazos. Esto debe estar orientado a objetivos y estrategias específicos. Tomando en cuenta el funcionamiento debe estar bien instalado y configurado desde la unidad respectiva del usuario.

Proceso de planeación de la auditoria

Debemos de evaluar y verificar las políticas, controles y procedimientos propios de las áreas administrativas, financieras, operativas, etc.

Con objeto de asegurar el buen manejo y administración de los recursos de la organización.

Orientados primordialmente al aseguramiento de la calidad y control de los diferentes elementos que se encuentran relacionados con los recursos de informática.

Planeación de auditoria informática

Para hacer una adecuada planeación de la auditoria en informática hay que seguir una serie de pasos previos que son permitirán dimensionar el tamaño y característica del área dentro del organismo a auditar, sus sistemas, organización y equipo. También podremos determinar el número y características del personal son de auditoria, las herramientas necesarias, el tiempo y costo así como definir los alcances de la auditoria para, en caso necesario poder elaborar el contrato de servicios.

Este proceso de planeación depende en gran medida del diagnóstico previo que lleve a cabo el auditor en informática sobre la situación que prevalece en cada una de las áreas o servicios de la función de informática.También se deben considerar las necesidades o prioridades que tenga la alta dirección de auditar o evaluar un área específica de informática.

Dentro de la auditoría general, la planeación es uno los pasos más importantes, ya que una inadecuada planeación provocará una serie de problemas que pueden impedir que se cumpla con la auditoria o bien hacer que no se efectué con el profesionalismos que debe tener cualquier auditor. Llevar a la práctica los conocimientos recibidos dentro de la materia de auditoria informática. Además, hacer un análisis del servicio de informática.

La planeación deberá ser documentada e incluirá:

- El establecimiento de los objetivos y el alcance del trabajo.
- La obtención de información de apoyo sobre las actividades que se auditaran.
- La determinación de los recursos necesarios para realizar la auditoria.
- El establecimiento de la comunicación necesaria con todos los que estarán involucrados en la auditoria.
- La preparación por escrito del programa de auditoria.
- La determinación de cómo, cuándo y a quien se le comunicaran los resultados de la auditoria.
- La obtención de la aprobación del plan de trabajo de la auditoria.

En el caso de la auditoria en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de varios objetivos.

- Evaluación administrativa del área de proceso electrónico.
- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr una adecuada planeación lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar.

Realizar un informe de auditoría con el objeto de verificar la educación de las medidas aplicada que se llevan a cabo a las amenazas.

Consideraciones para el plan de auditoria informática

- Diagnóstico de la situación actual. De los sistemas de información en operación.
- Debilidades. Que pueden motivar la auditoria de un sistema de información.
- Clasificación de riesgo. Que representa el uso de hardware y software en la organización.
- Evaluación del nivel de riesgo. Que representa el uso inadecuado de los productos y servicios por el personal de informática y usuarios dentro de la organización.
- Otros aspectos. Telecomunicaciones, EDI (intercambio electrónico de datos), automatización de proceso.
- Clasificación de los riesgos. Según criterios establecidos por la función de auditoria informática.

El proceso de planeación comprende el establecer:

- Metas.
- Programas de trabajo de auditoria.
- Planes de contratación de personal y presupuesto financiero.
- Informes de actividades.

Las metas se deberán establecer de tal manera que se pueda lograr su cumplimiento, sobre la base de los planes específicos de operaciones y de los presupuesto, los que hasta donde sea posible deberán ser cuantificables.

Los programas de trabajo de auditoria deberán incluir las actividades que se van a auditar, cuando serán auditadas, el tiempo estimado requerido, tomando en consideración el enlace de trabajo de auditoria planeado.(Echenique, Auditoria en Informatica, 2003).

Capitulo III Caso Práctico (COBAEM)

3.1 Marco Referencial

3.1.1 Antecedentes

El Colegio de Bachilleres del Estado de Michoacán fue creado por decreto de ejecutivo del estado el 13 de septiembre de 1983, con el objeto de impartir, impulsar, coordinar y normar, en la esfera de su competencia, la educación del nivel medio superior en el estado.

Sus primeros planteles se establecieron en las localidades de Huetamo, Jacona y Quiroga, a los que se agregó el plantel de Venustiano Carranza en diciembre del mismo año, sumando un total de 613 alumnos, distribuidos en 14 grupos, con una plantilla de personal integrada por 98 trabajadores.

Actualmente 1983 nació COBAEM a su creación, el colegio cuenta con 59 planteles y 19 extensiones que imparten estudios de forma escolarizada, 5 centros de tele bachillerato y 8 unidades del sistema de enseñanza abierta, lo que hace posible que el colegio de bachilleres tenga presencia en 87 poblaciones pertenecientes a 72 municipios de los 113 que comprenden el estado, lo que significa una cobertura del 63.7% de la geografía michoacana.

Con relación a la matricula, en el presente ciclo escolar 2005-2006 nuestro subsistema educativo atiende a 31 mil 859 alumnos, distribuidos en 666 grupos. De esta forma, el colegio de bachilleres se mantiene como la institución del nivel medio superior con mayor presencia educativa en el estado, al atender el 27% de la demanda en este nivel.

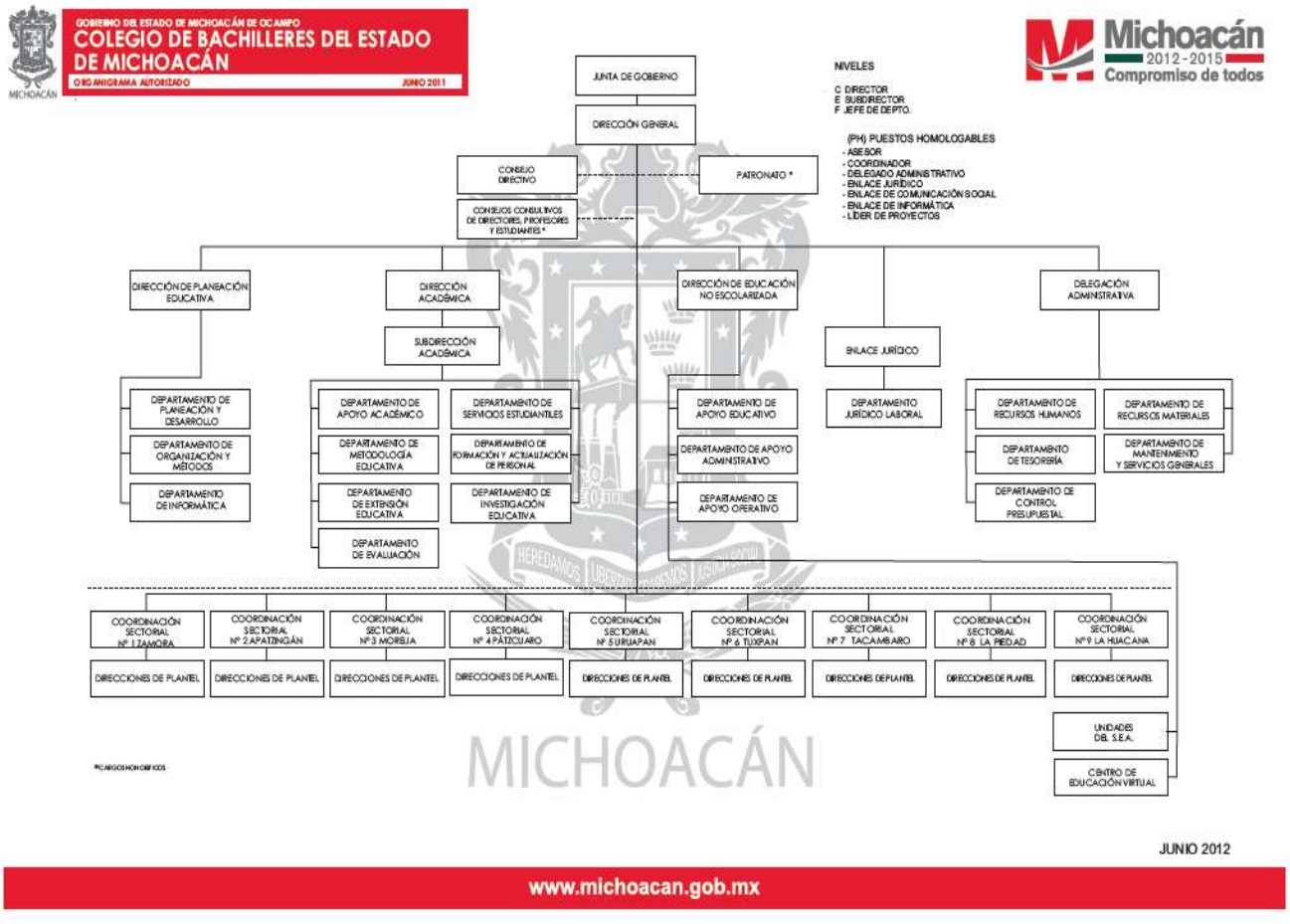
Estos y otros datos relevantes como infraestructura, equipamiento, plantilla de personal, información socioeconómica de las localidades en donde se ubican nuestros centros educativos, así como indicadores básicos de deserción, reprobación y eficiencia terminal, se presenta en la quinta edición de la estadística básica 2005-2006, con el propósito de aportar elementos que permitan dimensionar su importante cobertura e impacto en la educación de los jóvenes michoacanos.

Agradecemos la valiosa colaboración de los titulares de los planteles, unidades del sistema de enseñanza abierta y centros de tele bachillerato, por la información proporcionada, que hizo posible la integración de este documento.

3.1. 2 Giro

Se encarga de la educación donde ellos impulsan una educación media superior llevar el control administrativo institucional educativo como son los planteles, salarios de cada profesor, empleados de la misma institución, boletas de calificaciones y también de dar alta y baja de cada profesor. También considerando la información valiosa que tienen en el instituto COBAEM.

3.1.3 Estructura de la organización



3.1.4 Función del sistema del COBAEM

A través de profesionales de la educación, impartir e impulsar una educación media superior integral que asegura la formación de jóvenes comprometidos con su entorno, con amplio sentido de responsabilidad, críticos y propositivos, posibilitados para cursar exitosamente sus estudios superiores o insertarse en el mercado laboral.

El grupo de políticas de dominio se está implementando en el instituto del colegio de bachilleres del estado de Michoacán (COBAEM) trabajaremos con el servidor de dominio ya que con esto podemos restringir los programas, instalados los accesos de restringir a Windows. También así poder mantener en buenos términos nuestros equipos de cómputo y asegurarnos del despilfarro de información.

En la empresa COBAEM anteriormente el área de informática utilizaba el mantenimiento de las redes revisando los equipos manualmente y transándose de un lugar otro para habilitar o deshabilitar el internet, instalación de programas, bloqueo de los equipos etc. O checar que es lo que se estaba ocupando en el momento.

Actualmente estamos implementando y trabajando con los grupos de políticas, servidor de dominio. Qué se está trabajando con el servidor DNS en cual se realizar desde de una unidad, en donde todos los equipos están conectados a la misma red. Y si tener una mejorar la seguridad de toda la información requerida o cuenta el COBAEM, con nuestra información, amenazas y virus.

Las políticas de grupo del directorio activo se definen las configuraciones de grupos de usuarios y equipos, para controlar su acceso a los recursos de red. Utilizándolas se puede crear un entorno de trabajo que se adapte a las necesidades de cada usuario.

Ya que esto depende de las políticas que se requiera manejar en el servidor de la unidad.

El nivel de seguridad en el instituto de cobaem es de alta confianza ya que las políticas que manejan les permite a asegurar la información, las amenazas, de virus y robo de información, para autorizarles el permiso, a cada usuario en el instituto de COBAEM.

3.1.5 Metodología de auditoria en redes

Metodología de (Hernandez, 2000)	Metodología de (Piattini, 2001)
1. Estudio preliminar	1. Planeación
2. Revisión y evaluación de control y seguridad	2. Trabajos preliminares
3. Examen detallado de áreas criticas	3. Diagnostico administrativo
4. Comunicación de resultados	4. Investigación previa
	5. Elaboración del programa de la auditoria informática
	6. Obtención de información
	7. Análisis, clasificación y evaluación de la información
	8. Alcances y objetivos de la auditoria informática
	9. Estudio inicial del entorno auditable
	10. Determinación de los recursos necesarios para realizar la auditoria
	11. Elaboración del plan y de los programas de trabajo
	12. Actividad propiamente dichas de la auditoria
	13. Confección y redacción del informe final

De las 2 metodologías me pareció mejor y que esta mas completa fue la metodología de piattini, Mario para poder realizar el desarrollo de la auditoria.

3.1.6 Aplicación a la mejora de la metodología de la auditoria en redes

En base a la metodología podemos decir que es recomienda por (Piattini, 2001)

1. ***Planeación***

En el instituto de cobaem se pretende realizar la función de la información sea en tiempos a corto, mediano, y largo plazo. Para poder determinar la función de actividades en cobaem

El objetivo de **COBAEM** esbrindar formación integral de nivel medio superior a jóvenes y adultos a través de personal profesional capacitado, basada en un modelo educativo que propicie el desenvolvimiento pleno de las potencialidades del individuo, para lograr egresados competentes y comprometidos con el desarrollo social.

El nivel de seguridad en acceso.

El centro de cómputo **COBAEM** es mantener en buenos estados los equipos de cómputo para así mismo obtener un mejor logro en las actividades del trabajo y estar a tiempo todas las actividades realizadas durante el día. **COBAEM** de sea mantener y ofrecer un mejor servicio eficiente para el instituto.

Esto es con el fin de que todos nuestros movimientos realizados lleven un mejor control COBAEM. Así también podemos realizar, controlar y detectar más pronto las fallas de cualquier equipo de cómputo.

- Mantenimiento del equipo
- Habilitar o deshabilitar algún equipo que necesite el usuario

- Políticas

Una política de seguridad informática es una forma de comunicarse con el usuario, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

La política de la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización.

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

Objetivos de la política y descripción clara de los elementos involucrados en su definición.

Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.

Responsabilidades de los usuarioscon respecto a la información a la que tiene acceso.

Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.

- Controles

En el instituto de COBAEM están utilizando estos controles.

Controles preventivos: sirven para tratar de editar un evento no deseado de todas las áreas del departamento como son:Equipo de cómputo, Sistemas, Telecomunicaciones. Contar con un software de seguridad que impida los accesos no autorizados al sistema.

Controles Detectivos: trata de descubrir a posterior errores o fraudes que no haya sido posible evitarlos controles preventivos.

Controles Correctivos: trata de asegurar que se subsanen todos los errores identificados, mediante los controles preventivos; es decir facilitan la vuelta a la normalidad ante una incidencia.

El personal debe ser informado de la importancia de que participe en el esfuerzo de aplicar el control interno.

- Procedimiento

El objetivo de **COBAEM** es brindar los servicios para las inscripciones a los alumnos (as) de nuevo ingreso, a los profesores darles de alta a sus respectivas materias de cada uno de los profesor para que no de accedan de horas de trabajo.

El objetivo del centro de Cómputo de **COBAEM** es tener las bases de datos en perfectas condiciones para poder llevar a cabo cualquier trámite de los alumnos, profesores, pagos de los mismos profesores y empleados.

En el instituto de COBAEM están utilizando estos procedimientos

- Cuentas de usuarios
- Internet
- Correo Electrónico
- Claves de acceso o password
- Administrador de correo

Todo funcionario que tenga dudas acerca del material que puede enviar o recibir, debe consultarlo con su jefe inmediato

2. Trabajos preliminares

El centro de cómputo **COBAEM** su funcionamiento sistema información es la seguridad físicaque debe estar en buen estado los equipos de cómputo el cableado debe estar en buenas condiciones, así mismo la seguridad lógica que la bases de datos y toda la información obtenida este segura de cualquier contingencia que se presente.

3. Diagnostico administrativo

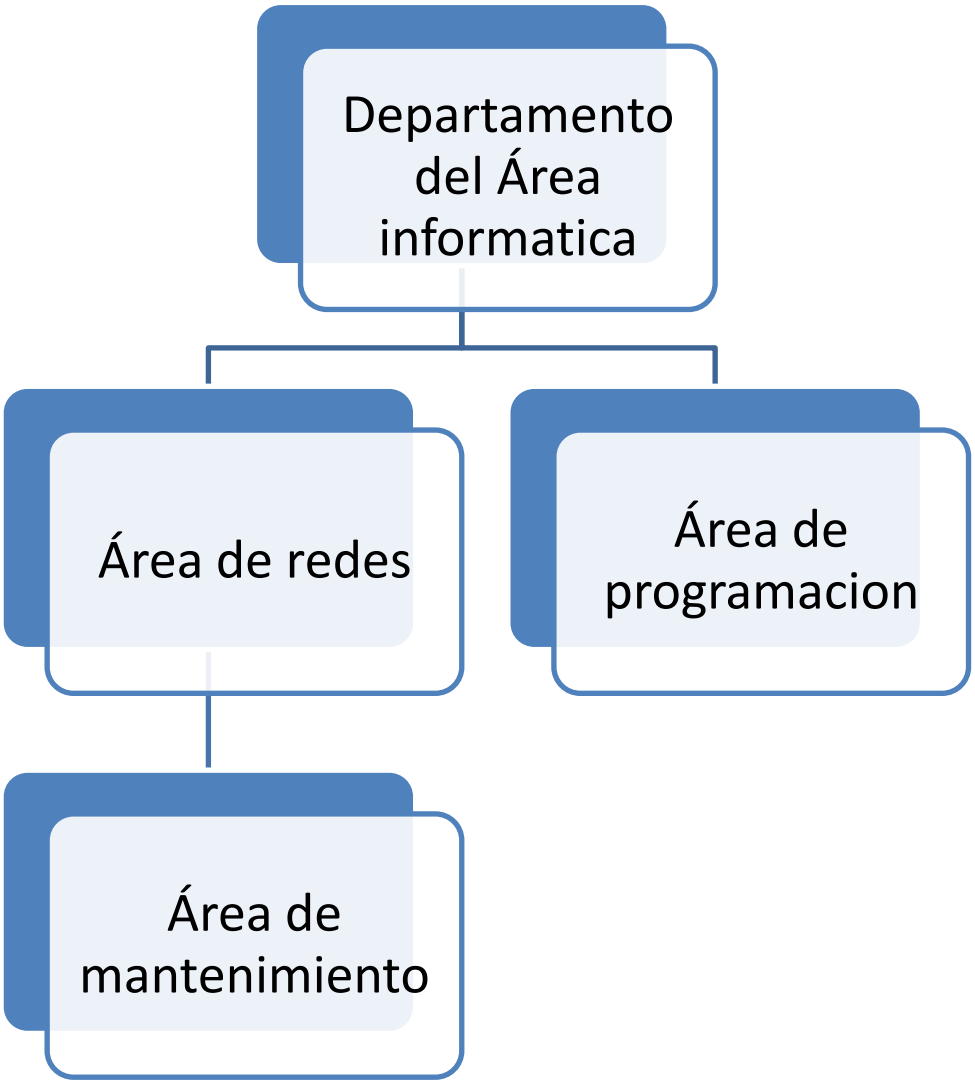
En el instituto de COBAEM se realizó una investigación de la estructura de organización en el área de informática, previa en donde ubicamos el del departamento de informática, que está ubicado en la tercera planta del edificio B en donde encuentra el departamento del área de redes.

4. Investigación previa

Con esto podemos decir que el centro de cómputo se encuentra en buen estado los mobiliarios, el funcionamiento del servidor DNS está funcionando de manera correcta, aunque se puede mejorar la seguridad que nos permite desde la unidad control a todos los usuarios, como habilitar y deshabitar cualquier irregularidad de algún equipo del usuario.

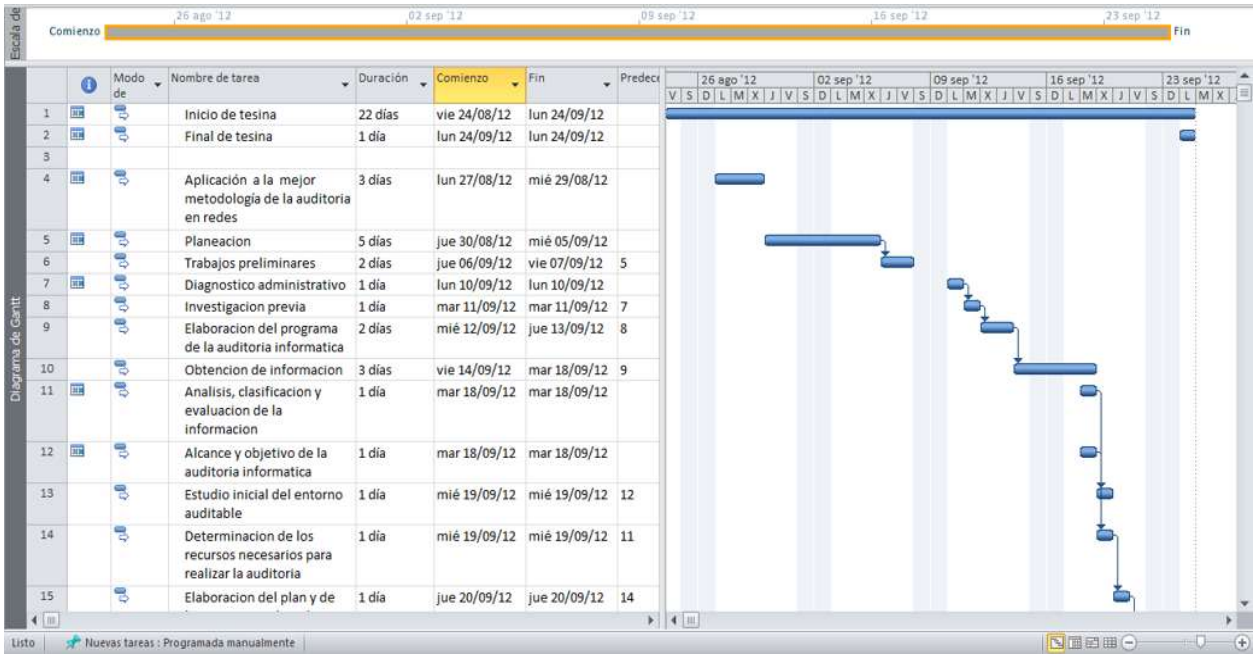
Centro de cómputo estos estructurados y conectado el cableado en perfectas condiciones para la red, y así tener una mejor seguridad de toda la información requerida.

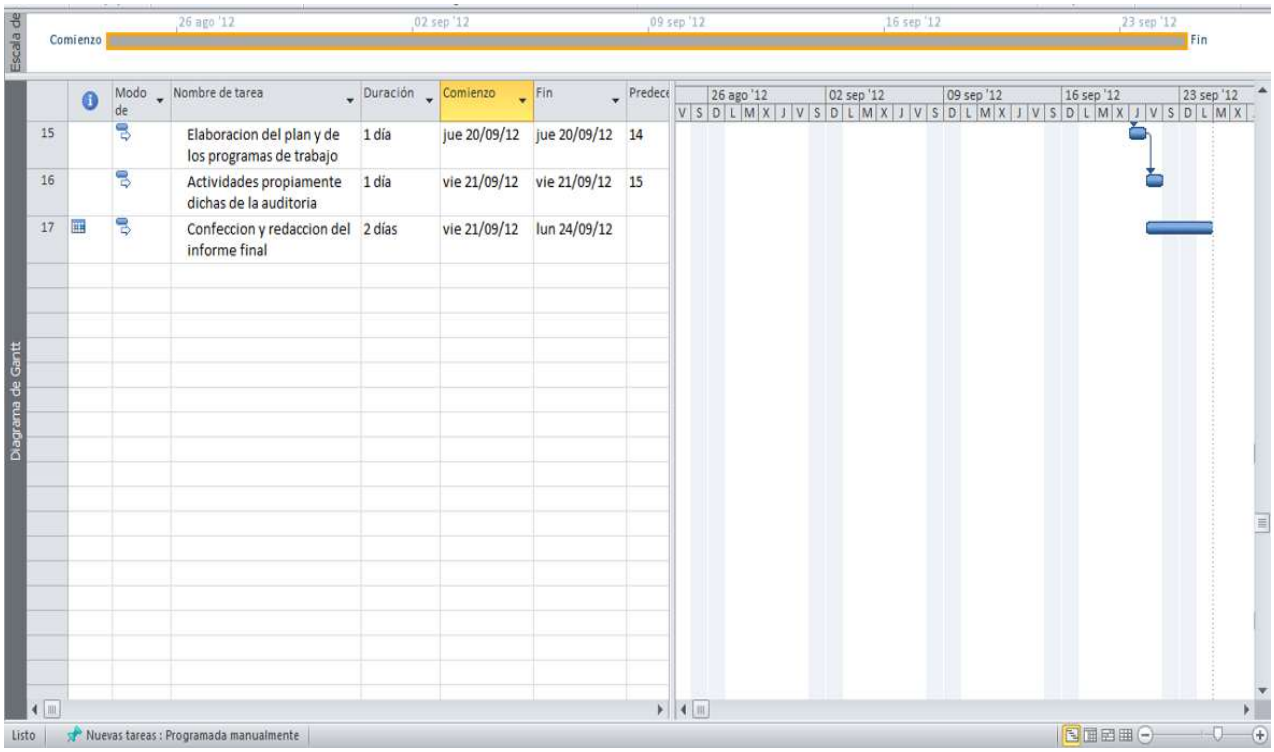
Un pequeño diagrama de los departamentos que están en el área correspondiente que se encuentra ubicado en la tercera planta del edificio B.


Departamento del Área informatica
Área de redes
Área de programacion
Área de mantenimiento

5. Elaboración del programa de la auditoria informática

Aquí realizamos un diagrama de Gantt





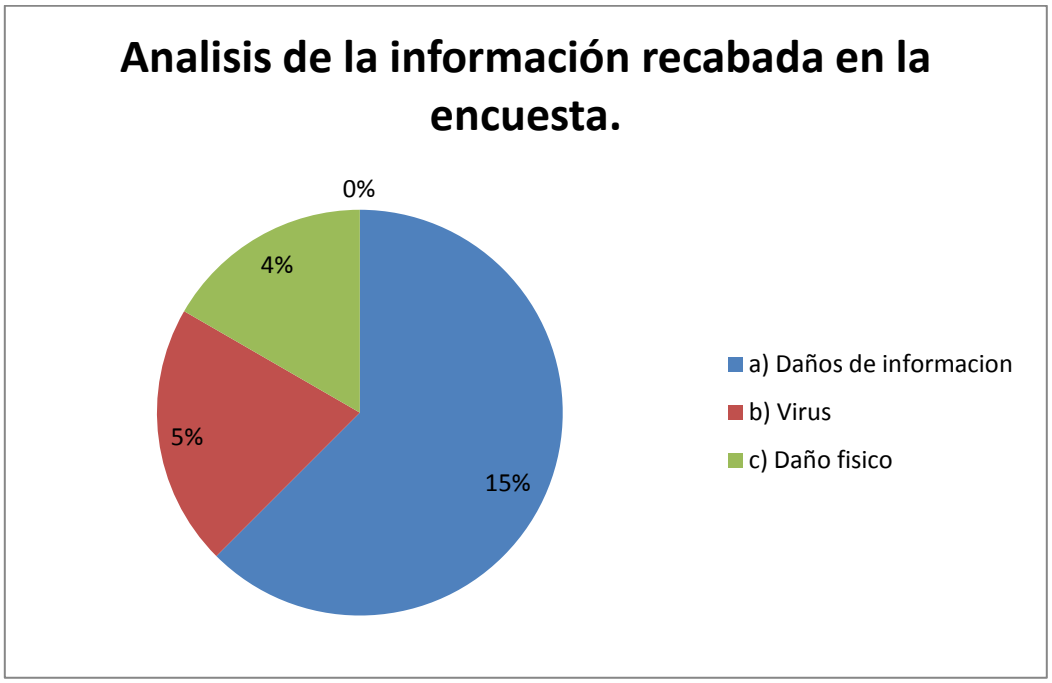
6. Obtención de información y análisis

Tomamos nuestra población de 100 empleados que colaboran en el instituto de COBAEM y el muestreo nos arrojó como resultado a 24 empleados, le realizaríamos el cuestionario.

La muestra fue de tipo de muestreo aleatorio. Siguiendo con el proceso de análisis de riesgo que se recomienda y se estructura el siguiente cuestionario.

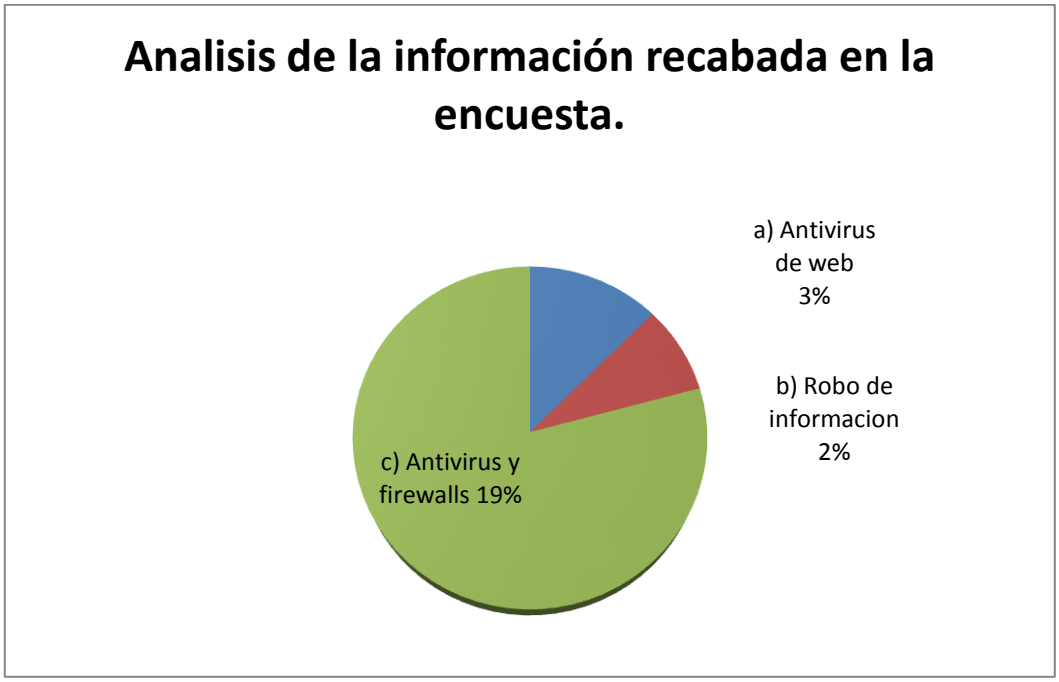
1. ¿Cómo podemos identificar y valorar las amenazas que puedan afectar a la seguridad de los activos?

a) Daños de información b) virus C) daño físico



2. ¿Cómo podemos prevenir el riesgo de amenaza y el robo de información?

a) Antivirus de web b) robo de información c) antivirus y firewalls



7. Análisis, clasificación de la información

- Objetivo
- Analizar los equipos de computo
- Que el auditor tenga experiencia y conocimiento
- Riesgos
- Riesgos de control
- Riesgo de detección

8. Alcance y objetivo de la auditoria informática

Este estudio se realizó únicamente al área de cómputo de COLEGIO DE BACHILLERES DEL ESTADO DE MICHOACAN. Y específicamente se revisó el riesgo que tenían en el centro de cómputo y en la administración de redes.

9. Estudio inicial del entorno auditable

Esto se hizo por la necesidad de llevar un mejor control en el COBAEM, así mismo poder identificar la problemática que estaba ocurriendo en el departamento del área de redes de COBAEM.

En el instituto de COBAEM son los riesgos más comunesque se van presentando en el traspaso de los días que van transcurriendo.

Amenazas y riesgo: son las amenazas más frecuente para cobaem ya que con estos riesgos es muy eficiente para poder tener el servicio que ofrece el instituto.

Robo de información: en el instituto de cobaem tiene que proteger mejor la información para que no sean robada.

Virus: para el instituto de cobaem tendrá que estar en constante actualización con sus antivirus, así evitar cualquier riesgo.

Dispositivos periféricos: le sirve para el instituto de cobaem para auxiliares e independientes conectados a la unidad central de procesamiento de una computadora.

Mal mantenimiento a los equipos de cómputo: para el instituto de cobaem sus equipos deben estar en buenas condiciones para poder realizar bien y eficientemente obtener los trabajo o las actividades este a tiempo en hora exacta que lo requieran en el instituto.

Despilfarro impresiones: en el instituto de cobaem tratara de evitar el despilfarro de impresiones, y será controlándolo desde el servidor DNS, con una cierta cantidad para cada usuario.

Riesgo: en el instituto de cobaem ante un posible o potencial perjuicio o daño para las personas y cosas, particularmente, para el medio ambiente. Tratar de prevenir los daños, para así mantener un mejor servicio eficiente y eficaz.

10. Determinación de los recursos necesarios para realizar la auditoria

Para poder realizar la auditoria o llevar a cabo el proyecto.

- 1 persona
- Equipo de cómputo
- Auxiliar
- Acceso a internet
- Papelería

11. Elaboración del plan y de los programas de trabajo

Es necesario conocer y determinar cómo se va realizar las actividades para poder llevar un orden en cada elaboración requerida.

1.- Planeación

2.- Trabajos preliminares

3.- Diagnostico administrativo

4.- Investigación previa

5.- Elaboración del programa de la auditoria informática

6.- Obtención de información

7.- Análisis, clasificación y evaluación de la información

8.- Alcance y objetivos de la auditoria informática

9.- Estudio inicial del entorno auditable

10.- Determinación de los recursos necesarios para realizar la auditoria

11.- Elaboración del plan y de los programas de trabajo

12.- Actividades propiamente dichas de la auditoria

13.- Confección y redacción del informe final

12. Actividades propiamente dichas de la auditoria

Tomar en cuenta a las personas quienes van a realizar la auditoria para la empresa de cobaem.

- Experiencia en el área de informática
- Técnico en informática
- Experiencia en operación y análisis de sistemas

13. Confección y redacción del informe final

De acuerdo al análisis realizado en los cuestionarios aplicados, a la encuesta de la empresa de **COBAEM**, nos podemos dar cuenta en qué situación se encuentra, el centro de cómputo. Por lo tanto consideramos que el tipo de dictamen es:

Salvedad

En la empresa de **COBAEM** la información fue muy limitada.
No hubo suficientes evidencias.

Corrección

Prevenir los activos de los diferentes tipos de riesgo tales como robo, incendios así como elementos naturales etc.

Recomendaciones

- ❖ Hacer un mantenimiento de rutina periódicamente en los equipos de cómputo.
- ❖ Cambiar periódicamente la contraseña de los equipos.
- ❖ Que tengan respaldo de toda información de la base datos periódicamente, cada quince días o por cada mes.

Conclusión

Durante este trabajo se logró observar que la seguridad de la redes es algo intenso en donde debemos estar día a día con las revisiones o manteniendo los equipos en buen estado ya que con el servidor de dominio se podrá llevar un buen control con toda la información.

También asegurarse del buen mantenimiento de los equipos para así tener un mejor uso de los equipos. Facilita realizar otras actividades en la empresa, y así mismo poder dar acceso a los usuarios a dicha información, o reinstrigirle, deshabilitar la información a los usuarios.

El objetivo esta tesina fue con la finalidad de proponer elementos de seguridad en redes para así poder tener la información al sistema más segura como también realizar el dictamen de auditoria y percatarse de las amenazas de cualquier virus que dañen los equipos de cómputo en **COBAEM**, con estos de servidores que utilizamos nos facilita verificar que todo esté en orden o funcionando correctamente el servidor de DNS.

El análisis del funcionamiento de la seguridad fue para tener un mejor control de la información y así mismo tener un respaldo de información para prevenir cualquier contingencia que se presente.

Para poder hacer una auditoria en perfectas condiciones se tubo que recurrir las metodologías así mismo poder realizar un diagnostico completo en nuestra auditoria.

El dictamen de diagnostico nos sirvió para darnos cuenta en que situación se encontró el centro de cómputo y nos permitió conocer la problemática mas común que son la amenazas de virus y de robo de información.

Los logros fueron favorables para la empresa ya que esto fue implementado en dicha empresa y los resultados son favorables.

La seguridad de la información está mejor protegida de cualquier sabotaje o robo.

Y esto nos es de mejo utilidad para la empresa ya que con esto podemos intervenir inmediatamente en deshabilitar cualquier anomalía que se presente en el instante, y así también como habilitar o dar permiso algún equipo de cómputo que necesite instalar algo urgente.

El servidor de DNS está funcionando factiblemente favorable.

En el instituto del COLEGIO DE BACHILLERES DEL ESTADO DE MICHOACA.

Bibliografía

Aguilera, L. P. (2010). *Seguridad Informatica y Comunicacion.* Mexico: Diana.

Bello, C. (07 de 2005). http://redalyc.uaemex.mx. *4*.

Echenique, G. J. (2001). *Auditoria Informatica.* Mexico: Mc Graw Hill.

Echenique, G. J. (2003). *Auditoria en Informatica.* Mexico: McGrawHill.

Fernandez, V. (2006). *Desarrollo de sistema de informacion .* España: Barcelona UPC.

FOROUZAN, B. A. (2002). *Transmision de Datos y Redes de Comunicacion.* MEXICO: Lisboa.

Hernandez, h. E. (2000). *Auditoria Informatica "Un Enfoque Metodologia".* Mexico: CECSA.

http://www.gestiopolis.com/Canales4/mkt/simparalas.htm. (s.f.). Recuperado el 26/08/12 de agosto de 2012, de http://www.gestiopolis.com/Canales4/mkt/simparalas.htm.

KENDALL, K. &. (2005). *Analisis y diseño de sistemas.* Mexico: Diana.

l. (s.f.).

Muñoz, C. (2002). *Auditoria en sistemas computacionales.* Mexico: Pearson Educacion.

Piattini, M. (2001). *Auditoria Informatica un Enfoque Practico.* Mexico: Alfaomegara.

Stallings, W. (2000). *Comunicaciones y Redes de Comunicacion.* Mexico: Lisboa.

Suarez, R. C. (2007). *Tecnologias de la informacion y la comunicacion : introduccion de los sistemas de informacion y de telecomunicacion.* Mexico: Vigo .

Yumar, A. (07 de 2008). *Modelo Informatica, para la Fisica.* Mexico: Diana.

Direcciones Electrónicas

http://www.eveliux.com/fundatel/menu_telecom.html
http://www.linti.unlp.edu.ar/trabajos
http://www.puertos.es/file?resId=1057575000105