ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERIA INFORMÁTICA CON ÉNFASIS EN GESTIÓN DE RECURSOS TECNOLÓGICOS.

"ELABORACIÓN DE UNA GUÍA DE AUDITORIA QUE PERMITA EL MEJORAMIENTO DE LA SEGURIDAD DE LA RED EN ELCENTRO AGRÓNOMO DE INVESTIGACIÓN Y ENSEÑANZA (C.A.T.I.E.)"

SUSTENTANTE

Esteban Zamora Delgado

Cedula 3-364-435

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO LICENCIATURA EN INGENIERÍA INFORMÁTICA CON ÉNFASIS GESTIÓN DE RECURSOS TECNOLÓGICOS.

PROF. Miguel Pérez Montero.

San José – Costa Rica

Agosto 2005.

RESUMEN EJECUTIVO DE LA INVESTIGACIÓN

El presente estudio pretende brindar una guía de auditoria a nivel cero en seguridad de redes para El centro Agrónomo de Investigación y Enseñanza (C.A.T.I.E.) esto con el fin de poder brindar los parámetros necesarios para identificar posibles vulnerabilidades, poder corregirlos, dar parámetros para proporcionar los valores para evaluaciones futuras a niveles más altos de auditoria. El departamento de cómputo del C.A.T.I.E no cuenta con una guía de auditoria en seguridad en redes, por lo cual se va a dar la primera guía de auditoria para que los encargados de dicha área elaboren el documento final en base a la guía proporcionada en el presente estudio.

La guía de auditoria esta elaborada en base a las normas que tienen influencia directa o indirecta en seguridad en redes que se presentan en el COBIT, el cual es una metodología que brinda los parámetros necesarios para elaborar guía de auditoria en sistemas de información. También se ha consultado bibliografía para así determinar los estándares, las normas, los procesos que se aplican y las técnicas modernas disponibles en materia de auditoria; así como la las herramientas, equipos y configuraciones más utilizadas en materia de seguridad de redes y la orientación en materia de seguridad en red que se maneja actualmente en el mundo.

Esta guía va servir de punto de partida para que el departamento de cómputo pueda auditar y así poder crear las rutinas de cada cuanto aplicar las guías de auditoria y el tiempo que se cuenta para poder corregir las deficiencias encontradas.

TABLA DE CONTENIDOS

CAPITULO I
Introducción

1.1 Introducción

La mayor parte de las organizaciones actuales necesita herramientas computacionales para llevar a cabo su funcionamiento normal, esta tecnología trae ventajas muy significativas para que las empresas cumplan con sus objetivos y metas, pero a la vez acarrea una serie de puntos de vulnerabilidad. Estas organizaciones cuentan con redes internas que necesitan conexiones con redes externas (Internet) por lo que aumenta las probabilidades de sufrir un ataque.

La forma más simple de proteger a una red interna contra peligros externos es aislándola físicamente y sin que exista posibilidad alguna de conectarse a ella remotamente. Sin embargo, un porcentaje significativo de la información que se requiere para el trabajo normal no se genera o está disponible en la organización, y por tanto es inevitable el acceso a entidades externas, que en términos de seguridad informática, pueden definirse como entidades no confiables. Estas conexiones a redes externas es una de las puertas más poderosas por donde las organizaciones pueden recibir ataques externos.

Sin embargo las empresas actualmente cuentan con una serie de herramientas de seguridad de red (software y hardware) para disminuir las posibilidades de que sean atacadas por intrusos, pero en muchas ocasiones las herramientas utilizadas no son las mejores o la forma de implementación no es la correcta.

El propósito de esta tesis es crear una guía de auditoria en políticas de seguridad en la red interna del C.A.T.I.E. que le permita chequear si todas las herramientas de seguridad de red están configuradas de una forma adecuada, además elaborar un Plan de general para definir los periodos en que se debe aplicar la auditoria.

1.2 Justificación

En la actualidad a nivel empresarial hay una fuerte competencia en todas las áreas, para que una empresa pueda competir en este mundo globalizado necesita implementar y utilizar herramientas tecnológicas. Una de las principales herramientas tecnológicas con las que cuentan las compañías son las redes tanto las privadas (Ethernet) como las publicas (Internet). Uno de los principales problemas con que se han enfrentado las redes de instituciones son los ataques por intrusos, que desean simplemente demostrar que pueden ingresar a la red privada, robar información o hacer un daño en la institución.

Las organizaciones cuentan con gran cantidad información muy vital para su funcionamiento diario, estas empresas para poder competir han optado por la utilización de herramientas tecnológicas. Esta misma tecnología que le trae tantos beneficios las organizaciones también acarrea puntos negativos como la vulnerabilidad de ataques a la red, por lo cual la seguridad se ha considerado como un punto de mucha importancia.

Las nuevas tecnologías que nacen diariamente han ayudado a que los ataques de intrusos a redes este aumentando significativamente y la empresas al no tener una guía clara de cómo poder evaluar si su red esta segura o no, a contribuido a este aumento.

Tomando en cuenta diferentes opiniones y lecturas realizadas las instituciones en los últimos años han optado por elaborar y realizar auditorias informáticas, muchas sin una metodología clara establecida, sin separar claramente las áreas (desarrollo software, Redes, hardware, software, etc.). A nivel de Red existe un desconocimiento acerca de una guía que realmente deben aplicarse para lograr administrar una red de forma segura.

Por esta observación que se decide investigar esta área, debido a que además de fomentar un crecimiento a nivel profesional, brindará un aporte importante al ofrecer una guía de auditoria sobre los aspectos de seguridad que deben ser cubiertos en las redes con exposición a Internet, para minimizar la posibilidad de una intromisión, lo cual es una contribución con relevancia social pues se estará protegiendo la información que cada empresa maneja, lo que es actualmente uno de los mayores valores con que las compañías cuentan y deben resguardar.

1.3 Planteamiento del Problema

EL Centro Agrónomo de Investigación y Enseñanza (C.A.T.I.E.), cuenta con una plataforma tecnológica bastante moderna, cuenta con servicios Web, correo electrónico (E-mail), bases de datos, correo interno, entre otros. Dentro del campo de las redes cuenta con una red interna (Ethernet) en todos sus diferentes edificios entre los que se pueden mencionar laboratorios, oficinas administrativos, habitaciones de los estudiantes, bancos, restaurantes, centros de investigación, bibliotecas, salas de conferencias y videoconferencias, entre otros.

Esta red interna cuenta con una conexión permanente a Internet muy necesaria en el funcionamiento diario de todos los miembros de la institución, motivo por el cual los accesos no deseados a la red, información perdida o dañada, equipo de software y hardware dañado va en aumento. La institución cuenta con gran cantidad de herramientas para proteger la red de ataques, pero no se cuenta con una guía de control interno que brinde

información acerca de qué tan segura está la red, ni qué metodología pueda utilizarse para una seguridad confiable.

El motivo del presente estudio es desarrollar una guía de auditoria que de el estado actual, y como poder corregir deficiencias encontradas en materia de seguridad de red, tema sobre el cual se conoce muy poco. Se realizará un manual de auditoria en donde se especificará las áreas y puntos críticos en donde se debe de aplicar o corregir la seguridad en la red, así como las formas de cómo poder solucionar las deficiencias.

1.4 Formulación del problema

¿Cómo puede mejorar la seguridad en la red del C.A.T.I.E. aplicando una guía de auditoria para tal efecto?

CAPITULO II
MARCO TEÓRICO

La auditoria en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. La auditoria en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Una auditoria en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

2.1 Metodologías de Auditoria

2.1.1 ISO 17799

Al ser la información de tan elevada importancia para las empresas, se comprende la necesidad de resguardarla del peligro de caer en otras manos y es por tal motivo que varios organismos internacionales se han dado a la tarea de estructurar normas o estándares para lograr de una manera uniforme proteger la información, entre estas existe la International Organization for Standardization (ISO), esta organización es bien conocida y está

encargada de fijar las normas aceptadas en Europa y en buena parte del mundo para así buscar la mayor compatibilidad de dispositivos y tecnologías, tanto en informática como en muchos otros campos. Por lo tanto la ISO especifica el estándar de seguridad informática ISO 17799.

La norma ISO 17799 no incluye la segunda parte de BS 7799, que se refiere a la implementación. ISO 17799 hoy es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían a elegir una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes.

Esta norma se subdivide en 10 áreas de control, las cuales se analizan a continuación.

Las diez áreas de control de ISO 17799

I. **Política de seguridad**: se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con soporte y dirección. La política también se puede utilizar como base para el estudio y evaluación en curso.
II. **Organización de la seguridad:** sugiere diseñar una estructura de administración dentro la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

III. **Clasificación y control de los recursos de información:** necesita un inventario de los recursos de información de la empresa y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

IV. **Seguridad del personal:** establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe tener presente implementar un plan para reportar los incidentes.

V. **Seguridad física y ambiental:** responde a la necesidad de proteger las áreas, el equipo y los controles generales.

VI. **Manejo de las comunicaciones y las operaciones:** los objetivos de esta sección son:

1. Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
2. Minimizar el riesgo de falla de los sistemas.
3. Proteger la integridad del Software y la información.
4. Conservar la integridad y disponibilidad del procesamiento y el envío de la información.
5. Garantizar la protección de la información en las redes y de la infraestructura de soporte.
6. Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
7. Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

VII. **Control de acceso:** establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

VIII. **Desarrollo y mantenimiento de los sistemas:** recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

IX. **Manejo de la continuidad de la empresa:** aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

X. **Cumplimiento:** imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento de la norma técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne la privacidad, la Ley de responsabilidad y transferibilidad del seguro médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Billey (GLBA por su sigla en inglés). Este segmento también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoria del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

2.1.2 COBIT

COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Misión: Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores

Usuarios:

- La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

- Los Responsables de TI: para identificar los controles que requieren en sus áreas.

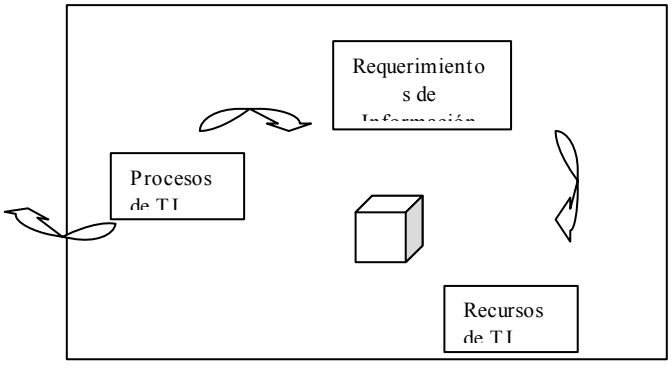
También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

Características:

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

Principios:

Figura 2.1.1 Principios de Cobit.



Esquema básico de los principios del Cobit
Fuente: Metodología Cobit.

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

- Requerimientos de la información del negocio

Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

Requerimientos de Calidad: Calidad, Costo y Entrega.
Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

- Efectividad: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
- Eficiencia: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
- Confiabilidad: proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
- Cumplimiento: de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.

Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad

- Confidencialidad: Protección de la información sensible contra divulgación no autorizada
- Integridad: Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
- Disponibilidad: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.
- Recursos de TI

En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

- Datos: Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.
- Aplicaciones: entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
- Tecnología: incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- Instalaciones: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

- Recurso Humano: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

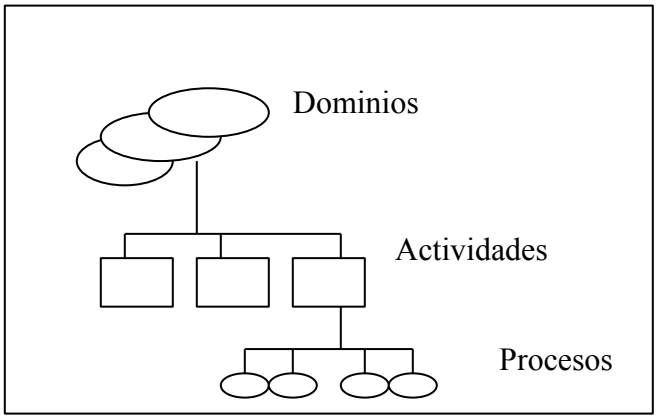
Procesos de TI

La estructura de COBIT se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".

COBIT se divide en tres niveles:

- Dominios
- Procesos
- Actividades

Figura 2.1.2 ***Niveles del Cobit.***



Esquema básico de los principios del Cobit
Fuente: Metodología Cobit.

Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.

Actividades: Acciones requeridas para lograr un resultado medible.

2.1.3 Proceso metodológico de la auditoria.

Una metodología de auditoria propone la descomposición del trabajo en seis etapas, de las cuales se extraen ciertos productos que a su vez son utilizados en las etapas siguientes. Las seis etapas con las cuales cuenta el proceso metodológico de la auditoria son:

1. Preliminar: Durante la etapa preliminar del proceso de auditoria se pretende conocer el grado de satisfacción que muestra la alta gerencia en relación con los servicios y productos ofrecidos por el departamento de tecnologías de información, así como analizar las áreas de oportunidad que se presenta en la organización en torno al departamento informático para convertir éste en un ente más competitivo y rentable dentro de la organización.

2. Justificación: Aquí se definen las áreas por auditar, se define el plan propuesto, se justifica la revisión o evaluación, y se obtiene el compromiso ejecutivo, que consiste en la aprobación para continuar con el desarrollo del proceso de auditoria.

3. Adecuación: se analiza y se llevan a cabo adaptaciones necesarias al proyecto para adecuarlo a las características presentes en la organización, sin dejar de lado todo lo

relacionado con los estándares y normas que rigen los procesos de auditoria tanto en el ámbito nacional como mundial.

4. Formalización: anteriormente se había obtenido un compromiso ejecutivo para continuar con el proceso, en esta etapa, se lleva a cabo la firma de un documento en el que se define la aprobación final de la auditoria y se da el inicio formal de la misma.

5. Desarrollo: es la puesta en práctica de todas las técnicas necesarias para el desarrollo de la evaluación del negocio, una vez que se finaliza el proceso, se elabora un informe de auditoria en el que se muestren los resultados encontrados durante todo el proceso.

6. Implantación: aquí se deben poner en práctica las recomendaciones hechas por el auditor en el informe entregado en la etapa anterior, se debe dar un seguimiento a las actividades realizadas, para corroborar que se están dando conforme a lo establecido y que se están obteniendo los resultados esperados.

2.1.4 Técnicas de auditoria.

Las técnicas de auditoria son los métodos prácticos de investigación y pruebas que se utilizan para la obtención y análisis de la información, y para la comprobación necesaria con el fin de emitir una opinión personal sobre un objeto estudiado. Entre las técnicas, que más comúnmente son utilizadas en los procesos de auditoria, según Cepeda (2000), las siguientes son algunas de las que pueden ser utilizadas para llevar a cabo auditorias.

Observación: se basa en el uso de los sentidos para la comprobación de que el desarrollo de los procesos u operaciones de la organización se están desarrollando de la forma correcta.

Inspección: consiste en la verificación técnica de un objeto en estudio, sus características, componentes, medidas, atributos técnicos, estado en que se encuentran, entre otros.

Revisión analítica: es una evaluación crítica, basada en la separación del ente estudiado en componentes de una manera organizada, por lo general se da para situaciones con cierto grado de complejidad.

Examen de exactitud: consiste en verificar la exactitud matemática teniendo en cuenta todas las características necesarias para poder llevar a cabo dicha verificación, esto sobre cualquier operación, documento o transacción.

Comprobación: se comprueba la veracidad de las transacciones realizadas mediante la obtención de evidencia suficiente que garanticen que se están desarrollando de la manera correcta y se ajustan a los criterios establecidos.

Conciliación: se establece la correspondencia y confiabilidad entre dos registros independientes, pero relacionados entre sí.

Análisis de saldos y movimientos: consiste en analizar el saldo de una cuenta en un estado financiero, identificando tanto los débitos y créditos que lo originaron, así como toda la documentación necesaria que los respaldan.

Confirmación: consiste en cerciorarse de la validez de las operaciones realizadas o de las cifras, mediante comunicación directa con terceros que conocen la naturalizar y condiciones de lo que se quiere confirmar.

Indagación: consiste en la identificación de las áreas débiles de los procesos mediante la obtención de información verbal extraída de los empleados y terceros.

Diagrama de flujo: consiste en describir en forma gráfica la secuencia de las operaciones de un ciclo de la entidad o de un proceso.

Estas técnicas se aplican a los diversos tipos de auditoria, algunas de ellas por su forma de obtener los datos, o bien por lo que se busca comprobar no es aplicado a todos los tipos de auditoria.

2.2 Seguridad en Redes

2.2.1 Firewalls

McClure, Scambrat y Kurtz (2002) exponen "Desde que Cheswick y Belovin escribieron su famoso libro sobre la construcción de cortafuegos y la persecución de un hacker llamado Berferd, la idea de conectar un servidor a la red de Internet (o cualquier otro equipo) sin utilizar un Firewalls se considera suicida" (p. 554).

Un Firewalls es un conjunto de componentes, ya sea un encaminador, un anfitrión, una combinación de encaminadores, computadoras y redes configuradas específicamente para proteger la información que fluye entre ellas, lo cual indica que un Firewalls refuerza la política de control de acceso entre dos redes.

También Quesada y Gutiérrez (2001) hacen referencia a que un Firewalls puede clasificarse dentro de uno de los siguientes tipos o como una combinación:

2.2.1.1) Filtrado de paquetes: el sistema de filtrado de paquetes encamina paquetes entre anfitriones internos y externos, pero de manera selectiva. Permite bloquear cierto tipo de paquetes de acuerdo con la política de seguridad de la red. El tipo de encaminamiento usado para filtrar paquetes en un Firewalls es conocido como encaminamiento de protección. El paquete es analizado detalladamente y se determina si éste puede ser encaminado o no a la dirección destino y si debe o no ser encaminado con base en la política de seguridad, realizar el encaminamiento y la decisión de encaminar es la única defensa del sistema. Si la seguridad falla, los servicios Web están expuestos. Un encaminamiento de protección puede permitir o denegar un servicio; no obstante, no puede proteger operaciones individuales dentro del servicio. Los Firewalls de este tipo trabajan a nivel de red, ya que, generalmente, toman las decisiones basándose en el origen, dirección de destino y puertos que leen en la cabecera de los paquetes IP. Ejemplos de un Firewalls de este tipo son:

2.2.1.1.a) **Firewalls de anfitrión protegido:** se accede a y desde un único anfitrión, el cual es controlado por un encaminador que está operando a nivel de red. El anfitrión es como una defensa, dado que está muy protegido y es un punto seguro para refugiarse contra los ataques.

2.2.1.1.b) **Firewalls de subred protegida:** se tiene acceso a y desde una red, la cual es controlada por un encaminador que opera a nivel de red.

2.2.1.2) Servicio Proxy: son aplicaciones o programas servidores intermediarios entre anfitriones internos de una red y los anfitriones de Internet de tal forma que reciben las requisiciones de unos y se las envían a los otros previa verificación de accesos y privilegios. Los Firewalls de este tipo trabajan a nivel de aplicación, pues generalmente son anfitriones que corren bajo servidores proxy que no permiten tráfico directo entre redes y que auditan el tráfico que pasa a través de ellas. A continuación se detalla un ejemplo de este tipo.

2.2.12.A) Gateway doblemente dirigido: es un anfitrión de alta seguridad que corre bajo Software proxy. Consta de dos interfaces de red -cada una se encuentra conectada a una red diferente-, éstas actúan generalmente como bloqueo o filtrador de parte o del total del tráfico que intenta pasar.

La mayoría de los servicios útiles son vulnerables. Su uso a través del Firewalls puede prevenirse, mientras que el uso interno está permitido. Un Firewalls puede proteger contra los ataques basados en la ruta y proveer autenticación para todos los accesos externos utilizando contraseñas de una sola vez. El Software de autenticación sólo tiene que ser instalado en los componentes del Firewalls y no en cada anfitrión. Un Firewalls puede ayudar a un lugar a ocultar información que puede ser útil a los intrusos. Además, puede mantener una auditoria de las conexiones de la red y puede detectar posibles intrusos.

Los Firewalls para seguridad están construidos en mecanismos que fueron desarrollados para otras funciones: encaminadores y gateways. Cada uno de estos

mecanismos conecta las redes y controla el tráfico de la red que pasa a través de él. Un encaminador utiliza una dirección de destino e instrucciones de direccionamiento posibles para determinar una ruta hacia el destino. Un gateway puede conectar dos redes que utilizan diferentes protocolos ya que puede traducir de un protocolo a otro.

Los componentes del Firewalls pueden ser manejados cuidadosamente. Un Firewalls no es un sustituto para una seguridad interna eficiente, pero puede adicionar una capa de protección ya que puede ser la única forma práctica para ganar los beneficios de una conexión de red.

2.2.2 Detectores de intrusos (IDS)

Se desprende que la detección de intrusos es el área aplicada de la seguridad informática encargada de informar de eventos que puedan tener lugar en un sistema informático y pueda ser considerado, por unas u otras razones, como parte de un intento de intrusión. Como intrusión se entiende elaborar un acto no autorizado, como puede ser el acceso a un sistema, la ejecución de programas no autorizados o el ataque a una red informática. El concepto de intrusión es cercano al de un ataque dirigido, pero algunas de las tareas previas a un ataque, como pueda ser la recopilación de información o la búsqueda de servicios, no están directamente tipificadas como ataque. Actualmente existe una controversia sobre si dichas actividades constituyen o no una actividad ilegal como lo pueda ser el acceso sin autorización a un sistema informático. El hecho de estar ante un entorno complejo, formado por un sistema de información global interconectado a través de

redes públicas de comunicación, hace difícil determinar si las actividades que realizan los sistemas por sí mismos pueden considerarse ataques cuando son realizados por personas con intención desconocida.

Un sistema de detección de intrusos ha de distinguir entre un acceso normal y habitual al sistema, que puede surgir de la puesta en marcha de servicios ofrecidos al exterior (entendiendo como exterior cualquier otro sistema ajeno al que ofrece los servicios), de un intento de vulnerar de algún modo dichos servicios, e incluso de aquellos que no debieran ser públicos, como parte del ataque a dicho sistema.

Es, por tanto, un sistema de detección de intrusos capaz de advertir al administrador de todas las situaciones que puedan ser consideradas como elementos o fases de una intrusión. El objetivo de dicho sistema es, en la medida de lo posible, proporcionar conocimiento de la puesta en marcha de un ataque sobre el sistema antes de que dicho ataque tenga éxito. Se ha de considerar como un mecanismo previo de alarma que está indisolublemente unido al mecanismo de respuesta. De esta, forma se podrán poner en marcha las medidas necesarias para mitigar el impacto.

Los sistemas de detección de intrusos quedan divididos en virtud, fundamentalmente, del lugar donde realizan la detección. Este lugar puede ser la red, basándose en el análisis del tráfico que pasa por ésta y su contenido, o puede ser el propio sistema operativo (basados en host) sobre el que se monitoriza el uso que las aplicaciones, procesos y usuarios hacen de él

2.2.3 Sistemas de red

Las redes cuentan generalmente con uno o varios servidores de red que son lo lugares donde se instala lo que se conoce como sistemas operativos de red, los cuales se encargan de muchas funciones y servicios en la red y, sin duda, la principal de ellas es velar por la seguridad mediante verificación de nombres de usuarios y contraseñas, así como mediante la asignación de permisos según privilegios del usuario en cuestión. Existe gran cantidad de sistemas operativos, entre ellos: Microsoft Windows 9x, 2000 Professional, XP, Windows 2000 Server, Windows .Net Server, Linux Red Hat, Linux Mandraque, Unix, etc.

2.2.4Vulnerabilidades

Cada uno de los sistemas expuestos anteriormente cuenta con vulnerabilidades, las cuales son utilizadas de muchas formas por los hackers para lograr entrar a las redes de datos desde Internet. Anteriormente, se comentó que exponer a un servidor o a cualquier otro dispositivo a Internet sin un Firewalls sería muy peligroso, pues según McClure et al. (2002):

Igualmente lo sería si se pone en manos del administrador de la red la tarea de su configuración, ya que generalmente estos no conocen a fondo la forma de actuar y pensar de los hackers, por lo cual puede resultar mal configurado permitiendo a los atacantes introducirse en la red.

Desde que se instaló el primer Firewalls, este tipo de dispositivos ha protegido innumerables redes de miradas curiosas y malintencionadas, pero están lejos de ser la

panacea de la seguridad. Cada año se descubren nuevos defectos en el terreno de la seguridad para cada uno de los Firewalls que aparecen en el mercado y, lo que es peor, la gran mayoría está mal configurado, carecen de mantenimiento y se encuentra sin vigilancia. No se debe creer que un Firewalls que cumpla con todas estas características será impenetrable, pues en realidad casi todos los hackers lo saben e intentarán entrar mediante relaciones de confianza y defectos en la seguridad de los enlaces más débiles o los evitarán totalmente lanzando un ataque mediante una cuenta de acceso telefónico. En resumen, la mayoría de los atacantes hacen casi cualquier cosa para evitar un Firewalls potente.

Casi todos los Firewalls emiten un "rastro" electrónico único; o sea, con una sencilla exploración de puertos de cortafuegos y captura de mensajes, los atacantes pueden determinar con efectividad el tipo, versión y reglas de casi todos los cortafuegos instalados en la red y al saber con exactitud cuál Firewalls existe en la red, resulta fácil empezar a buscar sus debilidades. La manera más fácil de buscar los Firewalls es mediante la exploración de puertos específicos predeterminados, lo único que necesita saber es qué buscar, por ejemplo, el Firewalls-I de Check Point escucha en los puertos TCP 256, 257, 258; mientras que el proxy Server de Microsoft suele escuchar en los puertos TCP 1080 y 1745, conociendo tal información, la identificación de estos tipos de cortafuegos es trivial si utiliza un explorador de puertos. Tanto los atacantes torpes como los audaces realizarán la exploración de su red de esta manera, buscando estos cortafuegos e intentando detectar cualquier resquicio en su armadura perimetral. Pero el más peligroso de los atacantes "peinará" su perímetro tan furtivamente como le sea posible.

Existen numerosas técnicas que los atacantes pueden emplear para no caer en su radar tales como ping aleatorios, puertos objetivos, direcciones objetivo y puertos origen; host de cebo; y realizar exploraciones de origen distribuido

A continuación se comenta acerca de las debilidades de los detectores de intrusos, tema expuesto por Fernández-Sanguino (2002), quien explica que la técnica tradicionalmente aplicada a la detección de intrusos, en todos sus ámbitos, consiste en el uso de reconocimientos de patrones para determinar ataques conocidos. De igual forma, la tecnología aplicada a la detección de virus, basada en la introducción de firmas más algunos heurísticos para detectar ligeras desviaciones, la detección de intrusos habitualmente busca en patrones que permiten discriminar un ataque de algo inofensivo.

Sin embargo, los problemas de la aplicación de esta técnica se pueden resumir en la incapacidad de detectar nuevos ataques: es decir, nuevos patrones. Esto deriva en que dichas herramientas han de ser actualizadas continuamente y que, además, siempre existirán ataques aún no descubiertos e identificados.

Existen dos condiciones por mencionar, una de ellas se denomina falsos positivos que es cuando se da la alarma de detección de ataques falsos, que en realidad son algunos patrones de accesos legítimos a los servicios. También están los falsos negativos que corresponden a ataques que pasan desapercibidos para el sistema de detección de intrusos. Cabe destacar que el segundo de estos problemas es, sin embargo, difícil de resolver en su totalidad debido a que, independientemente de la técnica empleada, siempre existirá un margen de error no nulo a la hora de clasificar un determinado evento como ataque o no.

El hecho de que los sistemas de detección de intrusos dependan intrínsecamente de las “firmas” que incluyen para detectar ataques es un grave problema a la hora de detectar ataques a aplicaciones que se acceden de forma supuestamente legítima.

Debido al auge de Internet se ha utilizado particularmente el protocolo http, como la forma de generar aplicaciones “a medida” independientes de plataforma al hacer uso de un elemento común, el navegador. Así, han surgido multitud de sistemas de gestión, de comercio electrónico, de información, etc., implementados sobre esta plataforma. Las aplicaciones utilizadas, no son generalmente productos adquiridos e instalados, sino que existe una gran heterogeneidad al tratarse, fundamentalmente, de utilidades realizadas a medida para las organizaciones, o de éstas para sus clientes.

El diseño de aplicaciones introduce nuevas vulnerabilidades dentro de los sistemas informáticos. Estas vulnerabilidades están habitualmente relacionadas con el tratamiento de los parámetros de entrada (datos de sesión, valores de formularios) que permitirán, con base en la implementación de la aplicación, posibilidades de ejecución de código arbitrario, ya sea dentro del sistema operativo del equipo, o bien en la aplicación mediante la ejecución de sentencias embebidas en el lenguaje de desarrollo (Java para los servidores de aplicaciones, Visual Basic para páginas ASP, PHP...). Evidentemente, los fabricantes de las herramientas de detección de intrusos no pueden proporcionar firmas para aplicaciones que desconocen, por esto habitualmente fracasan (entendiendo, como fallos, los falsos negativos) en la detección de estos ataques. Es posible, sin embargo, que los detectores de intrusos basados en host puedan detectar en cierta medida el comportamiento anormal de un sistema bajo ataque, lo cual dependerá sustancialmente de las acciones tomadas una vez que el sistema ha sido comprometido.

Para concluir se hace mención a la existencia de gran cantidad de errores de seguridad escritos en los millones de líneas de código fuente de cada sistema operativo, y aplicaciones en general, estos se descubren diariamente y de igual forma que en los casos anteriores, los hackers los utilizan para ingresar a las redes de datos desde Internet sin ser detectados. Se han expuesto sobre algunos sistemas de protección de redes de datos como los Firewalls, detectores de intrusos y seguridad en sistemas de red. No obstante, contar con ellos no asegura que la red esté protegida, aunque estén apropiadamente configurados. En el apartado “tipos de ataques” del anexo dos se puede ampliar el panorama actual de los ataques informáticos cuando se analicen los diferentes tipos que existen.

CAPITULO III
Marco Metodológico

3.1 Tipo de investigación

De acuerdo con la naturaleza, características y necesidades de información que muestra el presente estudio, referente al desarrollo de una Guía de Auditoria en Seguridad en Redes, orientado a investigar diferentes herramientas de seguridad en redes existentes, en el cual se pretende obtener información, propiamente del personal, de las bases de datos de la institución de C.A.T.I.E. y por encuestas, por lo cual esta investigación es de tipo descriptiva.

Lo anterior debido a que dentro de la investigación se pretenden conocer aspectos relacionados con Seguridad en redes Informáticas, así como los beneficios que se obtienen de una buena práctica de auditoria en Seguridad en Redes, a la vez que se busca especificar los parámetros que han de ser evaluados para la obtención de la información necesaria para el desarrollo del presente estudio.

Este trabajo será de tipo descriptivo, ya que se realizará una selección de las formas de seguridad más utilizadas, eficaces y eficientes, aplicadas en una auditoria de seguridad para una empresa en particular.

CAPITULO IV
Análisis de la situación Actual

El departamento de cómputo del C.A.T.I.E cuenta con un personal bastante capacitado en las distintas áreas en las que se da soporte como por ejemplo redes, mantenimiento de diversos equipos, bases de datos, aplicaciones, Web, entre otros. Dicho departamento es pequeño pero muy bien organizado, eficiente, muy planificado en todas sus actividades. Internamente cuentan con procedimientos para cumplir con cada uno de sus objetivos del departamento, uno de esos procedimientos es el de chequeo de la seguridad de la red

Procedimiento de chequeo de la Seguridad de la red del C.A.T.I.E

La institución del C.A.T.I.E. cuenta con un sistema de seguridad bastante eficiente y coordinado en todas sus áreas basado en tecnología y metodologías muy modernas, dicha seguridad se divide en dos grandes ramas: a nivel de Software y a nivel de Hardware.

Hardware

En esta área todo el equipo principal (servidores, routers, switch, firewall) se encuentran en cuartos con acceso restringido bajo llave, estos cuartos cuentan con todas las medidas de seguridad en cuanto a voltaje eléctrico, baterías, reguladores de corriente y aire acondicionado. El diseño y la distribución física de los cuartos han sido elaborados para que cada uno de los dispositivos tenga el espacio necesario para una adecuada manipulación por parte de los administradores.

Los switch de toda la red interna que se encuentran en las diferentes oficinas, salas de cómputo, residencias de los estudiantes, bibliotecas, entre otros, se encuentran en gabinetes con llave.

A nivel de Firewall la configuración es de carácter privado por medio del administrador de red, en su configuración se han utilizado todas las metodologías y estándares de seguridad vigentes recomendados por los fabricantes. Dicho Firewall cuenta con tres interfaces, una es la conexión hacia el Internet, otra con la zona desmilitarizada (DMZ) y la última hacia la red interna.

En la DMZ se encuentran todos los servidores que se pueden ver desde redes externas (Internet) y el Firewall bloquea el tráfico entrante según su fin por medio de puertos. Las estaciones que se detecten que están con tráfico muy pesado y que están saturando el ancho de banda son bloqueadas por medio de la dirección IP.

Al Firewall se le da mantenimiento cada dos meses en promedio, se revisan las bitácoras para observar su desempeño y posibles fallas.

Software

En esta área se cuenta con todas las políticas de seguridad que brindan los sistemas operativos a nivel de cuentas de usuario y protección de archivos. Cada usuario tiene su respectiva cuenta y contraseña de manera local, en otras palabras las cuentas de usuario están localmente en cada máquina, a nivel de los usuarios dueños de computadoras; en los centros de cómputo y computadoras de acceso público (lo utilizan muchos usuarios) se cuenta con una cuenta de usuario general (no administrador) para la utilización del equipo.

El software se revisa frecuentemente en todas las estaciones pero solo se revisa el software licenciado, eliminando el que no lo esté de ciertos usuarios y estaciones.

La red es totalmente abierta no por no contar con medidas de seguridad, sino por ser un centro de educación e investigación en donde se ocupa libre acceso. Cada usuario debe cambiar su password cada seis meses.

A nivel de respaldo de la información de los servidores se hace de manera automática todos los días de madrugada, estos respaldos se guardan en la misma oficina física en donde están los servidores, cada seis meses son llevados fuera, a las oficinas centrales de C.A.T.I.E.

CAPITULO V

Propuesta de listas de verificación de controles para la seguridad de la red del C.A.T.I.E.

Introducción

Una metodología para el auditoraje en la seguridad de redes en una institución ayuda a que en la red disminuya las posibilidades de una falla y accesos no autorizados y que las áreas que involucra o tiene relación con la red también disminuyan las posibilidades de falla.

Lo que se procura obtener con esta metodología es brindar una guía que le permita a los jefes del departamento Informático, encargados, técnicos y encargados de auditoria, realizar las actividades control exhaustivo, buscando dar un aprovechamiento más eficiente de los recursos y la obtención de una red segura.

Uno de los sustentos fundamentales del porque se desea ofrecer una guía que facilite el auditoraje en seguridad en redes se basa en que mientras más rápido se detecte el error y se corrige disminuyen los las deficiencias o posibles huecos de la red.

Dominio 1 Planificación y organización

Definición de un plan estratégico de Tecnología de Información

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo.

Entrevistas

Director General de Informática

Funcionarios principales de las distintas operaciones

Encargado de la red.

Encargado del departamento de cómputo

Control: Plan a largo plazo y mediano plazo de Tecnología de Información

Observaciones	Detalle de Prueba
¿Se han desarrollado e implementado Planes de largo y corto plazo de TI en función de los planes estratégicos de la Organización?	Solicite el plan de la organización y el de Tecnología de Información
¿El desarrollo de dicho plan se ha diseñado sobre la estructura de un plan estándar?	Solicite la estructura estándar establecida para realizar los planes y verifique que el de Tecnología de Información este confeccionado bajo este formato.
¿Se establece que el proceso de planeamiento del plan estratégicos TI, considere los resultados de la evaluación de riesgos tecnológicos?	Solicite la documentación que contenga las evaluaciones de riesgos tecnológicos efectuadas para la elaboración del plan estratégicos TI
¿Se realiza una evaluación, previa al desarrollo o modificación del plan de TI, de los sistemas existentes en términos de: automatización, funcionalidad, estabilidad, complejidad, costo, fortalezas y debilidades?	Solicite la documentación respecto a la evaluación de los sistemas existentes previo a la formulación del plan estratégicos TI
¿Se considera asimismo la incorporación de indicadores de ejecución y objetivos, con el fin de medir el grado de cumplimiento del Plan?	Verifique la incorporación de indicadores de ejecución en del plan estratégicos TI
¿Se ha desarrollado un proceso para reevaluar periódicamente y ajustar los planes de largo plazo de TI?	Solicite la documentación que respalde las modificaciones realizadas en el plan estratégicos TI
¿Se ha desarrollado un proceso para reevaluar periódicamente y de acuerdo a los cambios de planes de largo plazo se ajustan los de corto plazo?	Verifique que las modificaciones indicadas en el punto anterior hayan sido incorporadas dentro del plan estratégicos TI
¿Se realizan estudios de factibilidad para asegurar que la ejecución de los planes de corto plazo sean iniciados?	Solicite los estudios de factibilidad para 3 de los proyectos de corto plazo iniciados en este año.

¿Se comunican los planes de corto y largo plazo de Tecnología de Información, a los propietarios de los procesos y participantes relevantes de la organización?	Entreviste a 4 jefaturas de subprocesos y determine su conocimiento al respecto de los planes establecidos por Tecnología de Información

Definición de la Arquitectura de Información

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica,

Entrevistas

Director General de Informática
Funcionarios principales de las distintas operaciones
Encargado de la red.
Encargado del departamento de cómputo

Control: Planeación de la Infraestructura Tecnológica.

Observaciones	Detalle de Prueba
¿Existe un proceso para crear y actualizar periódicamente el plan de infraestructura tecnológica?	Solicite las políticas y los procedimientos referentes a la planificación y al monitoreo de la infraestructura tecnológica.
¿Los gerentes entienden y utilizan el plan de infraestructura tecnológica?	Solicite una explicación corta del plan de infraestructura tecnológica
¿Se compara el plan de infraestructura tecnológica con los planes de TI a corto y largo plazo?	Solicite el plan de Tecnología de Información y plan de infraestructura tecnológica

Control: Planes de adquisición de hardware.

Observaciones	Detalle de Prueba
¿La gerencia informática evalúa tecnologías emergentes e incorpora tecnologías apropiadas a la infraestructura existente?	Solicite los roles y las responsabilidades de dirección de los gerentes
¿Los planes de adquisición de hardware y software satisfacen, como norma, las necesidades identificadas en el plan de infraestructura tecnológicas?	Solicite el plan de infraestructura tecnológica y las normas de tecnologías aplicadas a la institución.
¿Se aplican normas de tecnología en relación con los componentes tecnológicos descriptos en el plan de infraestructura tecnológicas?	Solicite las normas de tecnología y compare con la infraestructura presente.

Administración de Recursos Humanos

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal.

Entrevistas

Director General de Informática

Funcionario y personal seleccionado de recursos humanos

Encargado del departamento de cómputo

Control: Capacitación del personal.

Observaciones	Detalle de Prueba
¿Existen planes de capacitación de personal?	Solicite las políticas y los procedimientos de capacitación de personal
¿Existen formularios de evaluación del desempeño y formularios de capacitación y	Solicite los descriptores de puestos, formularios de evaluación desempeño

desarrollo?	y formularios de capacitación.

Asegurar el cumplimiento con los requerimientos Externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales, para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos

Entrevistas

Director General de Informática

Asesores legales

Funcionario de recursos humanos

. Encargado del departamento de cómputo

Control: Cumplimiento de la normativa en materia de seguridad

Observaciones	Detalle de Prueba
¿Existen políticas y procedimientos en resguardos y objetivos de seguridad e higiene aplicables?	Solicite las normas de seguridad e higiene.
¿Los empleados están capacitados y educados en materia de seguridad e higiene?	Solicite los planes de capacitación de seguridad e higiene.
¿Hay criterios que determinen la criticidad de los datos que ingresan, procesan, almacenan, emiten y transmiten por la red?	Solicite políticas y procedimientos de criticidad de los datos
¿Existe procedimientos de seguridad de protección por contraseña y software para limitar el acceso a la red?	Solicite procedimientos de seguridad de la red.
¿Hay de seguridad en las terminales con acceso a la red?	Solicite procedimientos de seguridad de la red.
¿Existen medidas de encriptación de datos?	Solicite procedimientos de encriptación de datos.

¿Existen Firewalls en la red?	Entreviste al administrador de la red acerca de su existencia
¿Existen antivirus instalados?	Solicite la lista de los antivirus disponles y sus actualizaciones
¿Existen informes de violación de la seguridad de la red?	Revisar informes de violación de seguridad y su actualización.

Evaluación de riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos

Entrevistas

Director General de Informática

. Encargado del departamento de cómputo

Encargado de redes

Personal seleccionado de administración de riesgos

Control: Evaluación de riesgos

Observaciones	Detalle de Prueba
¿Existe un marco de evaluación de riegos sistemático que incorpora los riesgos de información relevante?	Solicite las políticas y los procedimientos referentes a la evaluación re riesgos.
¿El enfoque de la evaluación permite obtener periódicamente evaluaciones actualizadas a nivel global y especifico?	Revisar la evaluaciones de riegos hechas anteriormente

Control: Identificación de riesgos

Observaciones	Detalle de Prueba
¿Se disponen de procedimientos de evaluación de riegos a fin de determinar si los riesgos incluyen a factores internos o externos?	Solicite las políticas y los procedimientos referentes a la evaluación de riesgos.
¿Existen procedimientos para el monitoreo de evaluación de riesgos?	Revisar los procedimientos para el monitoreo de evaluación de riesgos.
¿El plan de evaluación de riegos cuenta con una descripción metodológica?	Solicite el plan de evaluación de riesgos.
¿El plan de evaluación de riegos identifica las exposiciones significativas y los riesgos correspondientes?	Solicite el plan de evaluación de riesgos.

Control: Medición de riesgos

Observaciones	Detalle de Prueba
¿Existe un enfoque formal cuantitativo y cualitativo (o combinado) para la identificación y medición de riegos, amenazas exposiciones?	Revisar la metodología utilizada a la hora de realizar y modificar el plan de riesgos
¿Los riegos, las amenazas y las exposiciones identificadas así como los atributos relacionados con los riesgos se utilizan para detectar cada aparición de una amenaza nueva específica?	Consultar la gerencia el procedimientos para detectar amenazas nuevas

Control: Plan de acción de reducción de riesgos.

Observaciones	Detalle de Prueba
¿Existen prioridades categorizadas desde la máxima hasta la mínima por cada riesgo existe una respuesta adecuada en el control preventivo para mitigar el riesgo?	Consultar el plan de acción de reducción de riesgos.

¿Existe un control secundario de detección de riesgos?	Consultar el plan de acción de reducción de riesgos.
¿Existe un control terciario de corrección de riesgos detectados?	Consultar el plan de acción de reducción de riesgos.

Dominio 2 ADQUISICIÓN E IMPLEMENTACIÓN

Adquisición y mantenimiento de la infraestructura tecnológica

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios, para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema

Entrevistas

Director General de Informática

Comité de planificación

.

Control: Evaluación del Hardware y Software nuevos.

Observaciones	Detalle de Prueba
¿Existen políticas y procedimientos de evaluación de hardware y software nuevo, a fin de determinar el impacto que pueden tener sobre el rendimiento general de la red?	Obtener las políticas y procedimientos utilizados para medir el desempeño del nuevo hardware y software en relación al antiguo.
¿La evaluación del desempeño se traduce en la comparación con los requisitos del sistema?	Comprar el desempeño del hardware en relación a los requisitos del sistema.

Control: Mantenimiento preventivo del Hardware.

Observaciones	Detalle de Prueba
¿Existen políticas y procedimientos para el mantenimiento preventivo del hardware a fin de reducir las fallas en su funcionamiento?	Obtener las políticas y procedimientos utilizados en el mantenimiento preventivo.
¿Se observan pasos y frecuencias en el manual de mantenimiento preventivo establecidos por los proveedores para cada dispositivo de hardware?	Localizar los pasos y frecuencias el manual de mantenimiento preventivo.
¿Existe un cronograma de mantenimiento preventivo?	Solicitar el cronograma de mantenimiento preventivo

Dominio 3: Prestación y soporte

Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado, para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos

Entrevistas

Director General de Informática

. Encargado de los servicios de información

Encargado de redes

Control: Requerimientos de disponibilidad y desempeño.

Observaciones	Detalle de Prueba
¿Los plazos y niveles de servicio de la red reflejan los requerimientos de los usuarios?	Solicite políticas y procedimientos referente a la disponibilidad, monitoreo e informes del desempeño, carga de trabajo , administración de la capacidad y listas de recursos
¿Los plazos y los niveles de servicio de la red están definidos para todos los servicios prestados?	Solicite políticas y procedimientos referente a la disponibilidad, monitoreo e informes del desempeño, carga de trabajo , administración de la capacidad y listas de recursos

Control: Plan de disponibilidad.

Observaciones	Detalle de Prueba
¿Existe un plan de disponibilidad, se aplica y refleja los requerimientos del usuario?	Solicite el plan de disponibilidad

Control: Monitoreo e informes.

Observaciones	Detalle de Prueba
¿Se lleva acabo un monitoreo permanente del desempeño y la capacidad de todos los equipos de la red?	Solicite el los informes de los monitoreos del desempeño de los equipos.
¿Existen los informes del desempeño destinados a los usuarios con la información sobre y uso y disponibilidad?	Solicite los informes del desempeño destinados los usuarios.

Garantía de seguridad de los sistemas.

Objetivo: salvaguardar la información contra usos no autorizados, divulgación, modificación, daño o pérdida, para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados

Entrevistas

Director General de Informática

Encargado de la seguridad Informática.

Encargado de redes

Control: Administración de las medidas de seguridad

Observaciones	Detalle de Prueba
¿Existe un plan estratégico de seguridad y control centralizado?	Solicite las políticas de seguridad de la organización y acceso a la red.
¿Existe una organización centralizada de la seguridad y es la responsable de garantizar el acceso adecuado de los recursos de los sistemas de información y de la red?	Solicite las políticas de seguridad de función de los servicios de información y acceso a los sistemas de información y a la red.
¿Existe un esquema de clasificación de los datos y se utiliza?	Solicite la forma en que clasifican la importancia de los datos.
¿Todos los recursos de la red tienen un responsable de la seguridad y su contenido? ¿Existen perfiles de seguridad del usuario y representa el mínimo de acceso requerido?	Ubique al encargado de la seguridad de los recursos de la red y solicite sus responsabilidades. Examine los diferentes perfiles de seguridad y sus niveles de seguridad.
¿La gerencia revisa periódicamente los perfiles de seguridad para su reacreditación?	Revisar las actas de las revisiones de los perfiles de seguridad.
¿Se tienen normas de administración de claves criptográficas?	Solicite las normas de administración de claves criptográficas.

¿Existen procedimientos para solicitar, establecer y mantener el acceso del usuario a la red?	Solicite los procedimientos de seguridad de la organización y acceso a la red.
¿Se lleva un inventario de los dispositivos de acceso a la red?	Solicite el inventario de acceso.
¿Existen informes referentes violaciones de seguridad en el campo de intentos no autorizados de acceso al sistema (Conexión)?	Solicitar informes.
¿Existen informes referentes violaciones de seguridad en el campo de intentos no autorizados de acceso a los recursos de la red?	Solicitar informes.
¿Existen informes referentes violaciones de seguridad en el campo de intentos no autorizados de visualizar o cambiar definiciones y reglas de seguridad? ¿Existen informes referentes violaciones de seguridad en el campo de cambiar privilegios de acceso a recursos por ID de usuario?	Solicitar informes. Solicitar informes.
¿Existen informes referentes violaciones de seguridad en el campo de cambios no autorizados de la definiciones y reglas de seguridad? ¿Existen informes referentes violaciones de seguridad en el campo de acceso autorizado a los recursos (seleccionados por usuarios o recursos)?	Solicitar informes. Solicitar informes.
¿Existen informes referentes violaciones de seguridad en el campo de cambio de estado de la seguridad del sistema?	Solicitar informes.

¿Existen informes referentes violaciones de seguridad en el campo de acceso a tablas de parámetros de seguridad del sistema operativo?	Solicitar informes.
¿El hardware y el software relacionados con la seguridad del la red, como los módulos criptográficos están protegidos contra violaciones o divulgaciones y el acceso está limitado?	Solicite las políticas de seguridad de la organización y acceso a la red.
Los procedimientos para la protección contra software malicioso incluye: -La verificación contra virus en todo el software adquirido. -Existencia de una política escrita sobre el uso del freeware y shareware y su cumplimiento. -Protección de software para aplicaciones extremadamente criticas mediante MAC. -Las instrucciones a los usuarios sobre la detección y los informes sobre virus. -Políticas y procedimientos para la verificación de medios extraíbles de virus.	Solicite las políticas de seguridad de la organización.

Control: Administración de las cuentas de usuario

Observaciones	Detalle de Prueba
¿Existen procedimientos de mantenimiento de claves y módulos criptográficos, su administración está centralizada y se utiliza para todas las actividades de acceso a la red?	Solicite los procedimientos de administración de usuarios, uso de criptografía y forma de administración.

¿Existen normas de administración de claves criptográficos?	Solicite si se tiene normas criptografía.
¿Los mecanismos de autentificación en uso presenta un solo uso de los datos de autentificación (por ejemplo las contraseñas no son reutilizadas)?	Solicite los procedimientos de administración de usuarios.
¿Los mecanismos de autentificación en uso presenta autentificación múltiple (por ejemplo se utilizan dos o más mecanismos de autentificación)?	Solicite las formas de autentificación.
¿Los mecanismos de autentificación en uso presenta autentificación basada en la política(es decir, la capacidad de especificar diferentes procedimientos e autentificación para eventos específicos)?	Solicite las formas de autentificación.
¿En el momento de identificarse aparece un mensaje de advertencia que le informa al usuario acerca del uso apropiado de hardware y de la red?	Solicite las políticas de control de acceso
¿Antes de completar la conexión de entrada, aparece una pantalla de advertencia que le informa al lector que un acceso no autorizado puede traer consecuencias jurídicas?	Solicite las políticas de control de acceso
La política de contraseñas incluye: -La imposición del cambio de contraseña inicial en el primer uso. -La extensión mínima de la contraseña. -La imposición de una frecuencia apropiada de cambios de contraseña. -La verificación de la contraseña en comparación con la lista de valores no permitidos.	Solicite las políticas de control de contraseñas.

-La protección adecuada de contraseñas de emergencia.	
Los procedimientos formales de resolución de problemas comprende: -La identificación de usuario se suspende luego de un determinado números de intentos consecutivos al iniciar sesión. -Se le muestra al usuario autorizado la fecha, la hora y cantidad de intentos infructuosos del último acceso, a la hora de iniciar sesión. -El tiempo de autentificación está limitado aun determinado lapso de tiempo, luego del cual se concluye la sesión.	Solicite los procedimientos de administración de usuarios.

Control: arquitectura de firewalls y conexiones de rede publicas.

Observaciones	Detalle de Prueba
El firewalls tiene las siguientes propiedades: -Todo el trafico desde adentro y hacia fuera y viceversa, debe de atravesar el firewall. -Sólo el tráfico autorizado, según las políticas de seguridad local, tendrá autorización de pasar. -El firewall es, en si mismo, inmune a penetración. - El tráfico se intercambia a través del Firewall sólo a nivel de aplicación. -La arquitectura del firewall combina las medidas de control tanto a nivel de aplicación como a nivel de red. -La arquitectura del firewall impone una	Solicite al administrador de red las políticas de configuración del firewall.

discontinuidad de protocolo a nivel de transporte. -La arquitectura del firewall debe de presentar una fuerte autentificación para la administración de sus componentes. -La arquitectura del firewall oculta la estructura de la red interna. -La arquitectura del firewall se define de ataques directos (por ejemplo, a través del monitoreo activo del tráfico y la tecnología de reconocimiento de patrones). -Todo el código ejecutable es escaneado para encontrar un código malicioso (por ejemplo virus, applets maliciosos) antes de que se introduzca a la red interna.	

Administración de instalaciones.

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

Entrevistas

Director General de Informática

Encargado de la seguridad informática.

. Encargado de administración de riesgos

Control: Seguridad física.

Observaciones	Detalle de Prueba
¿Las instalaciones están ubicadas en un lugar que no es visible desde afuera, se encuentran en un área mínimamente accesible y el acceso está limitado a una cantidad mínima de personas?	Solicite las políticas y procedimientos de administración de instalaciones, distribución, seguridad, lista de los individuos que tiene acceso.
¿Los procedimientos de acceso lógico y físico son suficientes, incluidos en los perfiles de acceso de seguridad de los empleados, proveedores y personal de mantenimiento?	Solicite las políticas y procedimientos de administración de instalaciones, distribución, seguridad.
¿Los procedimientos y las prácticas de administración claves y lectoras de tarjetas son adecuadas, actualizadas y revisados frecuentemente?	Solicite los mecanismos de entrada y salida y los procedimientos de mantenimiento de los mecanismos
¿Tiene lugar el proceso de revocación, respuesta y escalamiento ante una violación de seguridad?	Solicite los procedimientos de seguridad y procedimientos de vigilancia.
¿Las medidas de seguridad y control de acceso incluye dispositivos de información portátiles o dispositivos de almacenamiento utilizados en una sede externa?	Solicite los procedimientos de seguridad
¿Existe un acta de visitas? ¿Se efectúa la revisión de visitas, asignación de pases, acompañantes, persona responsable por las visitas?	Solicite el acta Solicite los procedimientos de seguridad.
¿Se lleva acabo la revisión de los procedimientos de advertencia y alarma de incendio, peligros climáticos y problemas eléctricos?	Solicite los procedimientos de seguridad

¿Se efectúa la revisión de los procedimientos de control de aire acondicionado, la ventilación, humedad y las situaciones de respuestas esperadas en distintos casos extremos de siniestro?	Solicite los procedimientos de seguridad
¿Se cumple con reglamentos en materia de seguridad e higiene?	Solicite los procedimientos de seguridad
¿Se aborda la seguridad física en el plan de contingencia y se garantiza que la seguridad física de la instalaciones?	Solicite el plan de contingencia.
Existen concretamente elementos alternativos de infraestructura que se necesitan para implementar la seguridad como: -Fuentes de alimentación de energía ininterrumpibles (UPS). -Tendido alternativo o nuevo enrutamiento de líneas de telecomunicaciones. -Recursos alternativos agua, gas, aire acondicionado.	Solicite el plan de contingencia.
¿Los gabinetes de conexiones están físicamente seguros con la posibilidad de acceso autorizado solamente?	Solicite los procedimientos de seguridad
¿La sala de servidores y de cómputo está separada y cerrada con llave y sólo accede a ella personal de operaciones?	Solicite los procedimientos de seguridad

CAPITULO VI
Conclusiones

A continuación se describen las conclusiones a las que se ha llegado al finalizar este trabajo de investigación sobre el desarrollo de una guía de auditoria en seguridad en redes en el Centro Agrónomo de Investigación Y Enseñanza (C.A.T.I.E.)

- **-Acerca de Centro Agrónomo de Investigación Y Enseñanza (C.A.T.I.E.).-**

El C.A.T.I.E. es una institución de enseñaza de estudios universitarios de postgrados en el cual se desarrolla una serie de proyectos de carácter científico. Cuenta con gran cantidad de estudiantes nacionales como internaciones. También en sus instalaciones cuenta con sedes de diferentes organizaciones, bancos, otras instituciones, agencias, pequeñas empresas, entre otros. Esta situado en Turrialba 4 KM carretera a Siquirres.

- **–Características que la hacen viable para el presente estudio-**

EL Centro Agrónomo de Investigación y Enseñanza (C.A.T.I.E.), cuenta con una plataforma tecnológica bastante moderna, cuenta con servicios Web, correo electrónico (E-mail), bases de datos, correo interno, entre otros. Dentro del campo de las redes cuenta con una red interna (Ethernet) en todos sus diferentes edificios entre los que se pueden mencionar laboratorios, oficinas administrativos, habitaciones de los estudiantes, bancos, restaurantes, centros de investigación, bibliotecas, salas de conferencias y videoconferencias, entre otros. Dicho departamento de cómputo no cuenta una guía de auditoria de redes para chequear un corregir posibles deficiencias.

- **-Metodología Utilizada para la elaboración de la Guía-**

La guía de auditoria está elaborada en base a los objetivos que se plantean en el Cobit en relación a sistemas de información, de dicha metodología solo se utiliza los puntos de control que tiene relación con la seguridad en redes. Se utiliza en cobit debido a que la guía de auditoria que utiliza la parte de la gerencia de C.A.T.I.E. esta desarrollada en base a Cobit, y además que cobit es una metodología bastan nuevo con metodologías moderna y muy eficiente.

- **-Estado de la guía en seguridad en redes-**

Debido a que el departamento de redes no cuenta con ninguna guía de auditoria en seguridad en redes, los puntos desarrollados en la guía son a un nivel cero, lo que se pretende en este nivel cero es identificar las deficiencias y que los encargados de auditoria desarrollen la guía definitiva en base a esta guía y en lo resultados obtenidos, dando ya las calificaciones en base a las necesidades y el grado de criticidad.

- **-Ciclos en que se debe aplicar la guía y como corregir las deficiencias-**

Los ciclos que se debe aplicar la auditoria deben de ser discutidos con la gerencia informática en los cuales de tiempo para corregir los errores y que se comience un nuevo ciclo para aplicar la guía nuevamente.

Bibliografía

Cepeda, Gustavo (2000). *Auditoria y control interno.* Colombia: McGraw Hill.

Comité de dirección del Cobit y fundación de auditoria y control de sistemas de información (1998). *Pautas de auditoria;* Recuperado el 19 de abril de 2004, de www.cobit.com

Comité internacional de prácticas de auditoria (2001). *Normas internacionales de auditoria*. México.

Delgado, Xiomar (1998). *Auditoria Informática*. San José, Costa Rica: Editorial EUNED.

Diccionario Océano Uno. (1991). Bogotá Colombia: Editorial Grupo Editorial Océano.

Elaboración de un esquema de seguridad (2003). Recuperado el 22 de Febrero 2005, de http://www.delrina.com/region/mx/enterprisesecurity/content/framework/LAM_573.html .

Echenique, José A. (2001). *Auditoria en Informática*. México: Editorial McGraw-Hill. 2ª Edición.

Fernández-Sanguino Peña, J. (2002). Sistemas de detección de intrusos: carencias actuales y nuevas Tecnologías*. Revista Seguridad. Sistemas de detección de intrusos 49*. 1 - 3

Li, David (1990). *Auditoria en centros de cómputo*. México: Editorial Trillas.

La necesidad de un sistema de detección de intrusos(2003). Recuperado el 22 de Febrero 2005, Http://www.delrina.com/region/mx/enterprisesecurity/content/expert/LAM_MP001_html2

Microsoft (2004). Technet Seguridad. Recuperado el 3 de Marzo de 2005, de http://www.microsoft.com/latam/technet/articulos/articulos_seguridad/marzo/seguridad- basica- ***Firewalls***.asp.

Piattini, Mario y Del Peso, Emilio (1998). *Auditoria Informática: un enfoque práctico.* Colombia: RA- MA Editorial.

Revista CONECtronica (2002). Seguridad con cortafuegos Parte I. Recuperado el 22 de Febrero 2005, de http://www.conectronica.com/articulos/seg23.htm.

Revista CONECtronica (2002). Seguridad con cortafuegos Parte II. Recuperado el 22 de Febrero 2005, de http://www.conectronica.com/articulos/seg24.htm.

ANEXOS

Anexo Nº 1

INSTRUMENTO N° 1 Entrevista
Universidad Latinoamericana de Ciencia y Tecnología
Investigación para optar por el grado de Licenciatura en Ingeniería Informática, con énfasis en Gestión de Recurso Tecnológicos
Realizado: Jefe de Departamento de informática del C.A.T.I.E
Fecha: _____.
Revisado: Esteban Zamora.
Objetivos: Identificar las principales formas de ataques no deseados que han sido perpetradas en la red del C.A.T.I.E.
Objetivo de la entrevista: Obtener información concisa y veraz del Jefe de Departamento informática del C.A.T.I.E, de las herramientas de seguridad de Red implementadas.

1) ¿Qué lugar tiene la seguridad de la red en el C.A.T.I.E?

A) Muy alta.
B) Alta.
C) Poca.
D) Muy Poca

2) ¿Qué marcas utiliza en Hardware y/o Software de seguridad de red? ¿Por qué?
_____
_____
_____
3) ¿Qué tipo de información es la que está protegiendo?
_____
_____
_____

4) ¿Cuales son los tipos de ataques más frecuentes?
_____
_____
_____

5) ¿Cuál es la frecuencia con la que se le da mantenimiento a las herramientas de seguridad de red?
_____
_____
_____

6) En términos de tiempo y trabajo ¿cuánto se tardaría poner en línea todos los servicios Web y correo electrónico luego de una caída? ¿Cuántas personas se verían afectadas en sus labores?

_____
_____
_____

7) ¿Podría haber otras implicaciones en caso de una caída o hurto de Información? Explique

_____
_____
_____

8) ¿Conoce acerca de vulnerabilidades o puertas traseras existentes en sus sistemas de seguridad? ¿Cuáles? (menciones dos o tres). (Si la respuesta es sí, pase a la pregunta 9; de lo contrario vaya a la pregunta 10)

_____
_____
_____

9) ¿Cómo las ha cubierto para evitar ser penetrado por ahí?

_____
_____
_____

10) ¿Qué sistemas operativos se utilizan?

_____
_____
_____

11) ¿Qué fallas presentan los sistemas operativos instalados a nivel de seguridad?

_____
_____
_____

12) ¿Se siente realmente protegido con su plataforma de seguridad?
Explique

_____
_____
_____

13) ¿Utiliza sistemas de detección de intrusos? (Si la respuesta es sí, pase a la pregunta 14; de lo contrario vaya a la pregunta 16)

_____
_____
_____

14) ¿Cuál o cuales sistemas de detección de intrusos utiliza y porque?

_____
_____
_____

15) ¿Cuáles son las principales fallas los detectores de intrusos? ¿Cómo se ha solucionado el problema?

_____
_____
_____

16) ¿Ha considerado asistencia externa? (Si su respuesta es sí indique cuál situación de estas: auditoria, configuración, atención de Contingencias)

_____
_____
_____