AUDITORIA INTEGRAL DE SISTEMAS A LA CORPORACIÓN UNIVERSITARIA UNITEC

OSCAR JAVIER BAUTISTA BELTRÁN
NIYARETH MARCELA MAYORGA URREGO

Trabajo de grado para optar al título de Tecnólogo en Sistemas

Asesor
Gustavo Adolfo Cruz Pineda
Ingeniero de Sistemas

CORPORACIÓN UNIVERSITARIA UNITEC
ESCUELA DE INGENIERÍA
TECNOLOGÍA EN SISTEMAS
SECCIÓN DE AUDITORIA
BOGOTÁ D.C.
2005

AUDITORIA INTEGRAL DE SISTEMAS A LA CORPORACIÓN UNIVERSITARIA UNITEC

OSCAR JAVIER BAUTISTA BELTRÁN
NIYARETH MARCELA MAYORGA URREGO

CORPORACIÓN UNIVERSITARIA UNITEC
ESCUELA DE INGENIERÍA
TECNOLOGÍA EN SISTEMAS
SECCIÓN DE AUDITORIA
BOGOTÁ D.C.
2005

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del asesor

_____
Firma del jurado

_____
Firma del jurado

Bogotá, Julio 15 de 2005

A mis padres, Pedro Bautista Y Maria Eugenia Beltrán por su constante apoyo y comprensión incondicional en todos los momentos de mi vida para poder llegar a este punto,
A mis abuelas, tíos, primos y amigos por sus aportes y enseñanzas.
Los amo mucho.

A mis padres Isauro Mayorga y Teresa Urrego, por su constante apoyo, soporte, motivación y orientación en mi vida.
A mi hermano Jair y mi tía Gilma por acompañarme en todo momento y brindarme sus aportes
A Diego Camilo Gómez Por su valiosa compañía y consejos en esta etapa de mi vida, a mi familia, amigos y compañeros. Los amo mucho

AGRADECIMIENTOS

Expresamos nuestros más sinceros agradecimientos a:

Profesor Gustavo Adolfo Cruz Pineda por su iniciativa en el área de auditoria de sistemas, y su constante orientación, supervisión y motivación en este proyecto de grado.

Ingeniero de la Universidad de las Villas de Cuba Manuel Oliver Tovar por sus valiosos aportes en el desarrollo de la auditoria de red, apoyo incondicional y orientación durante la investigación.

Funcionarios del Departamento de Informática de la Corporación Universitaria Unitec por su colaboración para el desarrollo de la auditoria Integral de sistemas.

A las personas que tuvieron contacto durante la ejecución del proyecto.

A las familias Bautista Beltrán y Mayorga Urrego por su apoyo incondicional y contribución para lograr con éxito nuestro proyecto de grado.

A nuestros amigos y compañeros mas cercanos.

TABLA DE CONTENIDO

Capitulo 1
INTRODUCCIÓN

1.1 ANTECEDENTES

Se tiene evidencia que algún tipo de auditoria se practicó en tiempos muy remotos, ya que los soberanos exigían el mantenimiento de las cuentas de su residencia por dos escribanos independientes, se pone en manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrollo el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales. La auditoria como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la Ley "Un sistema metódico y normalizado de contabilidad era deseable para una adecuada información y para la prevención del fraude". También reconocida como "Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas". Desde 1862 hasta 1905, la profesión de la auditoria creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia el 1900. En Inglaterra se siguió haciendo en cuanto a la detección del fraude como objetivo primordial de la auditoria.

En los que podrían llamarse los días en los que se formó la auditoria, a los estudiantes se les enseñaba que los objetivos primordiales de ésta eran:

- La detección y prevención de fraude.
- La detección y prevención de errores.

Sin embargo, en los años siguientes hubo un cambio decisivo en la demanda del servicio, y los propósitos orientándose a:

- Evaluar la condición financiera actual y de las utilidades de una empresa.
- La detección y prevención de fraude, siendo éste un objetivo menor.

Este cambio en el objetivo de la auditoria continuó desarrollándose, no sin oposición, hasta aproximadamente 1940. En este tiempo "Existía un cierto grado de acuerdo en que el auditor podía y debería no ocuparse primordialmente de la detección de fraude". El objetivo primordial de una auditoria independiente debe ser la revisión de la posición financiera y de los resultados de operación como se indica en los estados financieros del cliente, de manera que pueda ofrecerse una opinión sobre la adecuación de estas presentaciones a las partes interesadas.

Paralelamente al crecimiento de la auditoria independiente en los Estados Unidos, se desarrollaba la auditoria interna y del Gobierno, lo que entró a formar parte del campo de la auditoria. A medida que los auditores independientes percibieron la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoria independiente, se mostraron partidarios del crecimiento de los departamentos de auditoria dentro de las organizaciones de los clientes, que se encargaría del desarrollo y mantenimiento de unos buenos procedimientos del control interno, independientemente del departamento de

contabilidad general. Progresivamente, las compañías adoptaron la expansión de las actividades del departamento de auditoria interna hacia áreas que están más allá del alcance de los sistemas contables. En nuestros días, los departamentos de auditoria interna efectúan evaluaciones sobre todas las áreas corporativas, en donde las operaciones financieras forman parte.

La auditoria gubernamental fue oficialmente reconocida en 1921 cuando el Congreso de los Estados Unidos estableció la Oficina General de contabilidad. Legislaciones posteriores ampliaron y clarificaron su autoridad, particularmente con respecto a las corporaciones del Gobierno, pero la legislación sentó la base primaria para ampliar el alcance de la auditoria, abarcando más allá de la contabilidad, asuntos financieros y cumplimiento legal.

El objetivo de BSA (Business Software Alliance) es erradicar la piratería informática trabajando en tres aspectos fundamentales: La educación, la promoción de legislaciones que protejan los derechos de la propiedad intelectual y las acciones legales. [1]

[1] www.gestiopolis.com/recursos4/docs/fin/apuestaud.pdf (15 de marzo de 2005)

1.2 JUSTIFICACIÓN

Es necesario medir la efectividad del sistema de control interno informático determinando riesgos que puedan afectar la integridad del personal, equipos e información, brindando así, oportunidades de mejora en cada uno de los aspectos evaluados.

Con el fin de dar una solución a esta problemática, se plantearan alternativas para la eficiencia en el uso de recursos informáticos y la relación costo-beneficio, incremento el nivel de satisfacción de los usuarios de los sistemas computarizados y contribuir en mejorara la seguridad, integridad, confidencialidad y confiabilidad de la información mediante recomendaciones a las directivas de la Corporación Universitaria Unitec y sus áreas técnicas.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Efectuar una auditoria integral de sistemas a la Corporación Universitaria Unitec con el fin de evaluar la red informática, estructuras físicas y el sistema de información general SIG.

1.3.2 OBJETIVOS ESPECÍFICOS

- Evaluar el nivel de rendimiento, seguridad, distribución, control de mantenimiento preventivo y correctivo de la red tanto lógico, físico y administrativo.
- Evaluar los aspectos físicos de la instalación tecnológica sede C de la Corporación Universitaria Unitec.
- Aplicar un seguimiento evaluativo al modulo de admisiones del sistema de información general SIG, que se encuentra en desarrollo actualmente en Unitec verificando el cumplimiento de cada una de las fases del ciclo de vida del sistema.

1.4 PLANTEAMIENTO DEL PROBLEMA

Actualmente la Corporación Universitaria Unitec dispone de una red de información, instalaciones físicas y un sistema de información en desarrollo, aspectos sobre los cuales no se observa seguimiento evaluativo sistemático.

Es decir se desconoce la efectividad del sistema de control interno y del esquema de seguridad implementado para estos componentes tecnológicos.

Capítulo 2
CONCEPTOS GENERALES DE AUDITORIA

2.1 CONCEPTO DE AUDITORIA

Es un examen crítico, sistemático y representativo del sistema de información de una empresa o parte de ella, realizado con independencia y utilizando técnicas determinadas, con el propósito de emitir una opinión profesional sobre la misma, que permita la adecuada toma de decisiones y brindar recomendaciones que mejoren el sistema evaluado.

La "American Accounting Association" [AAS, 1972] con un criterio más amplio y moderno define en forma general la Auditoria identificándola de la siguiente manera:

La Auditoria es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso. [1]

De acuerdo a lo anterior la auditoria la definimos como un control destinado a evitar errores por negligencia y/o irregularidades dentro del funcionamiento de los distintos entes u organizaciones. Por ello cuando se habla de auditoria en un sentido general se entiende que implica examinar o revisar determinado objeto o

[1] http://members.tripod.com/ (11 de Marzo de 2005)

atributo. Todo ente u organización, ya sea con fin de lucro o sin él, posee ciertos controles o parámetros preestablecidos para permitir su habitual funcionamiento. La auditoria controla dichos parámetros, razón por la cual, en forma rudimentaria, se suele decir que la auditoria es el control de los controles existentes en el ente auditado.

2.1.1 TIPOS DE AUDITORIA POR ENFOQUE

Entre los principales enfoques de auditoria tenemos los siguientes:

Financiera: Veracidad de los estados financieros y preparación de informes de acuerdo a principios contables.

Operacional: Evalúa la eficiencia, la eficacia y economía de los métodos y procedimientos que rigen los procesos de una empresa.

Sistemas o Informática: Se preocupa de la función informática y tecnológica.

Fiscal: Se dedica a observar el cumplimiento de las leyes fiscales.

Administrativa: Analiza los logros de los objetivos de la administración y el desempeño de funciones administrativas.

Calidad: Evalúa métodos, mediciones, controles de los bienes y servicios de acuerdo a normas y estándares predefinidos.

Social: Revisa la contribución a la humanidad así como la participación en actividades socialmente orientadas.

2.2 AUDITORIA INFORMÁTICA

La auditoria en informática es la revisión y la evaluación de los controles, sistemas y procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, para que a través de cursos alternativos se logre un aprovechamiento más eficiente y seguro de la información y la tecnología facilitando los procesos de 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.

La 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, redes y comunicaciones y la gestión de la dirección). [1]

2.2.1 TIPOS DE ENFOQUE DE AUDITORIA INFORMÁTICA

Auditoria Física: La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los

[1] http://www.gerencie.com/auditoriasistemasinformacion.htm (11 de Marzo de 2005)

albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Auditoria a Aplicativos en Desarrollo: Verificación y observación de las metodologías implementadas, control interno de las aplicaciones, satisfacción de usuarios, diseño, análisis orgánico (preprogramacion y programación), pruebas e implementación. La auditoria en este caso deberá principalmente comprobar la seguridad de los programas en el sentido de garantizar que lo ejecutado por la máquina sea exactamente lo previsto o lo solicitado inicialmente.

Auditoria a Aplicativos en Funcionamiento: Evaluación y validación de datos de entrada y salida de un modulo o software que se encuentre operando.

Verifica la concepción de los programas, en esta fase se examina operando, sometiéndolos a ejecuciones con datos reales, para poder confrontar las salidas con aquellas que, en su día, obtuvo el ordenador en su normal proceder. Es importante que el juego de datos a procesar permita verificar todos los posibles caminos de los programas, haciendo incluso especial incidencia sobre determinados puntos críticos o delicados. Ello se simplifica si los programas están debidamente estructurados, lo que facilitará enormemente la detección de errores, o las posibles modificaciones. Los datos podrán ser grabados nuevamente, en cuyo caso, además, se verifica la fase de grabación, o se utilizarán tal y como los tenga la empresa en los soportes de almacenamiento externo.

Auditoria de sistemas Operativos: 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. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas.

Auditoria de Red: Una auditoria de red permitirá a una empresa comprobar el estado de su instalación de red, desde la electrónica hasta los protocolos de transmisión para las diferentes aplicaciones, pasando por los problemas de las políticas de seguridad aplicadas.

Auditoria a Bases de Datos: Se evalúan las metodologías utilizadas para el Diseño de la Base de Datos y los distintos entornos que se utilizan.

El auditor debe analizar la metodología de diseño para determinar si es o no aceptable, debe tener en cuenta el diseño lógico y físico determinando estructura, relaciones, restricciones, especificaciones de almacenamiento y seguridad.

Auditoria a la Dirección Informática: Es una evaluación que se realiza a la(s) persona(s) encargada(s) de llevar el control del área de informática. Examina la eficiencia de los sistemas verificando el cumplimiento de la normativa general de la empresa y revisa la eficacia de la gestión de los recursos materiales y humanos informáticos.

Auditoria Forense: Busca apoyarse en la recolección de evidencia, investigación de fraudes informaticos y divulgación de información secreta.

2.3 AUDITORIA INTEGRAL DE SISTEMAS

Es una evaluación completa que comprende dos o más enfoques de auditoria informática para aplicarse en una empresa u organización.

Esta auditoria tiene como objetivo mejorar la relación costo-beneficio de los sistemas automáticos y computarizados, de igual forma poder asegurar la confidencialidad y confiabilidad de la información mediante unas recomendaciones de seguridad y controles.

Esta evaluación se lleva acabo teniendo en cuenta los distintitos enfoques que existen dentro de la auditoria informática.

La auditoria integral de sistemas que se realizó en la Corporación Universitaria Unitec cubrió:

- **Auditoria de Red** (física, lógica y administrativa)
- **Auditoria de Aplicativos en Desarrollo** (modulo de admisiones)
- **Auditoria Física** (Sede C)

Capítulo 3
PLAN Y PROGRAMA DE AUDITORIA INTEGRAL DE SISTEMAS

3.1 PLAN DE AUDITORIA

ÁREA FUNCIONAL: Área de Sistemas de la Corporación Universitaria Unitec.

APLICATIVOS Y PROCESOS SUJETOS A EVALUAR:

1. **Auditoria de Red:** Evaluación y análisis de la Red Informática de la Corporación Universitaria Unitec en la parte (Física, Lógica y Administrativa).
2. **Auditoria de Aplicativos en Desarrollo:** Evaluación y Análisis del aplicativo Sistema de Información (SIG).
3. **Auditoria Física:** Evaluación y observación de las instalaciones de los laboratorios de informática de la sede C.

A. OBJETIVO GENERAL:

Evaluar, a través de una Auditoria Integral de Sistemas, las condiciones físicas, lógicas y administrativas de la red, evaluar el sistema de información SIG y las instalaciones de la sede C.

Emitiendo un concepto que aporte valor y facilite los procesos de mejoramiento continuo sobre los componentes tecnológicos de unitec.

De acuerdo con los estándares que se deben tener en cuenta para cada una de las de las auditorias expuestas anteriormente.

B. ALCANCE DEL TRABAJO DE AUDITORIA:

La auditoria Integral De Sistemas se realizara a partir del 27 de febrero del 2005 hasta el 30 de julio del 2005, los aspectos a evaluar serán:

- La auditoria de red pretende evaluar la condición física, lógica y administrativa, del Área de Sistemas. la cual comunica las distintas sedes de la universidad por medio de su red, así mismo acceso al centro de computo, seguridad y reglamento del administrador, de igual forma la distribución del cableado.
- En la auditoria al sistema de información SIG se evaluara el buen funcionamiento de este nuevo software para la universidad, así mismo se tendrá en cuenta para la evaluación las fases de diseño del ciclo de vida del sistema.
- Para la auditoria física pretende evaluar las condiciones de infraestructura de la sede C, en la cual se encuentran los laboratorios de informática de la Corporación Universitaria UNITEC, así mismo, los controles de acceso a ella y a los equipos. De igual forma la ubicación del centro eléctrico, las condiciones de seguridad tales como rutas de evacuación y planes de prevención y atención de incendios e inundaciones.

C. CONOCIMIENTO DEL ÁREA SUJETA A EVALUACIÓN

En el área de sistemas de la corporación universitaria unitec reposan todos los equipos de red que prestan el servicio de comunicación entre las distintas sedes,

allí mismo se encuentra las personas desarrolladoras de software para la corporación universitaria unitec.

La Sede C está destinada para el uso de los laboratorios tanto de sistemas como los de electrónica y diseño por parte de la comunidad Uniteista.

1. Esquema Administrativo y/o Funcional

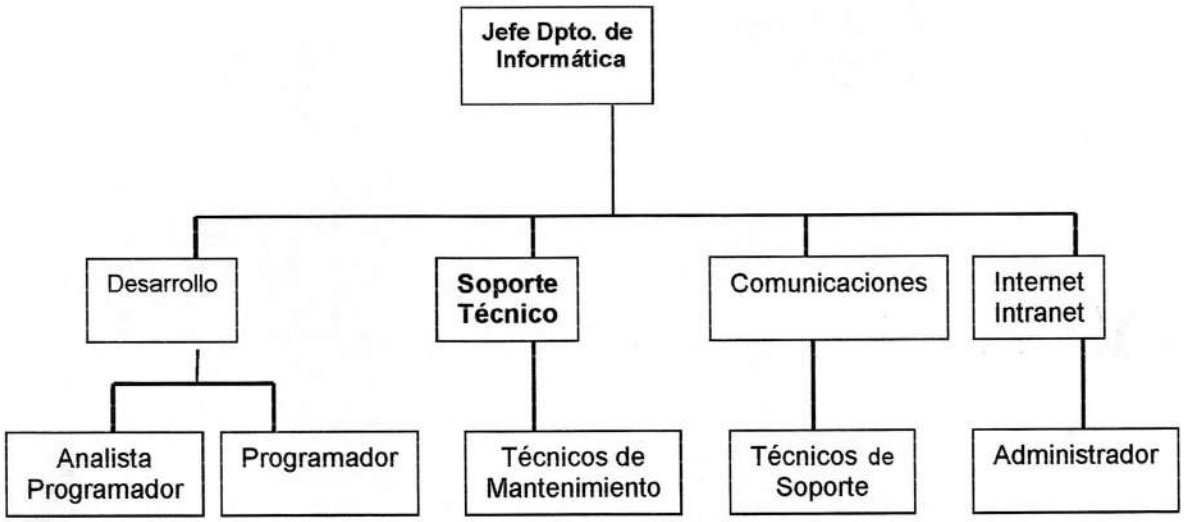

Figura 3.1: Organigrama departamento de sistemas

2.1. Cuestionarios o Derroteros de Auditoria.

Realizar y aplicar las entrevistas y encuestas necesarias al personal encargado de la red, desarrolladores del sistema de información y personal encargado de la sede C.

2.2. Principales Clientes / Usuarios:

Los principales clientes son todas las personas que hacen uso de los recursos que brinda la Corporación Universitaria Unitec, lo cual la universidad esta en la

condición de brindar un beneficio, que es la comunidad Uniteista que comprende desde el personal que trabaja allí hasta los estudiantes.

D. PERSONAL A INVOLUCRAR EN EL DESARROLLO DE LA AUDITORIA.

Equipo Auditor:

Niyareth Marcela Mayorga	Auditor de sistemas
Oscar Javier Bautista	Auditor de sistemas
Gusta Adolfo Cruz	Asesor

Personal Unitec:

Cesar Chisica	Ing. SISTEMAS
Jorge Saboya	Ing. SISTEMAS
Edgar Chamorro	Ing. SISTEMAS
Héctor Javier Piedras	PROGRAMADOR
Oscar Castañeda	ADMINISTRADOR
Luis Guillermo Vélez	JEFE DE SEGURIDAD
Ever German	CORDINADOR DE SEGURIDAD

3.2 PROGRAMA DE AUDITORIA INTEGRAL DE SISTEMAS

A. OBJETIVO GENERAL

Evaluar, a través de una Auditoria Integral de Sistemas, las condiciones físicas, lógicas y administrativas de la red, el sistema de información SIG y las instalaciones de la sede C.

Emitiendo un concepto que aporte valor y facilite los procesos de mejoramiento continuo sobre los componentes tecnológicos de unitec.

De acuerdo con los estándares que se deben tener en cuenta para cada una de las de las auditorias expuestas anteriormente.

B. OBJETIVOS ESPECÍFICOS

- Evaluar el nivel de rendimiento, seguridad, distribución, control y mantenimiento preventivo y correctivo de la red tanto lógico como físico y administrativo.
- Evaluar los componentes tecnológicos y las instalaciones físicas de la sede.
- Realizar un seguimiento valorativo al sistema de información SIG que se encuentra en desarrollo actualmente en Unitec revisando que satisfaga los requerimientos y que considere las etapas del ciclo de vida de un sistema de información.

C	ACTIVIDADES PARA LA AUDITORIA DE RED.
	AUDITORIA FÍSICA:
1	Conocimiento del área de sistemas.
2	Conocimiento de la red, entrevista al administrador de la red
3	Análisis de la documentación de la red.
4	Visita al área de sistemas, conocimiento de los componentes tecnológicos
5	Evaluación al acceso físico al cuarto de maquinas (servidores, swhitct, etc.)
6	Evaluación del medio ambiente en donde se encuentra el centro de computo
7	Entrevista o cuestionario con el personal que brinda soporte a la red.
8	Análisis de documentación para la operación de la red (manuales, notas internas, etc.)
9	Observación y análisis del cableado de la red.
10	Analizar y observar la seguridad de los equipos tecnológicos de la red (hardware)
11	Análisis y verificación del cumplimiento de los estándares y normas IEEE y ANSI/TIA/EIA dentro de la red.
	AUDITORIA LOGICA:
12	Evaluación y observación del acceso lógico a los equipos.
13	Evaluación lógica de la seguridad de la red.
14	Entrevista al administrador, para conocer la transmisión de datos.
15	Evaluación y verificación sobre los registros de las actividades de los usuarios de la red.
16	Analizar y evaluar los diferentes procedimientos que se utilizan para la instalación de hardware y software ilegal.
17	Evaluar y observar si se hacen simulaciones de ataques a la red.
	AUDITORIA ADMINISTRATIVA.
18	Asegurar que exista una administración formal de la red.
19	Entrevista al administrador, sobre los procedimientos y tareas que realizan cada uno de los jefes inmediatos del área de sistemas.
20	Verificar la existencia de manuales que indiquen las actividades y funciones del personal responsable de la red.
21	Analizar los resultados obtenidos en el proceso.
22	Evaluar y analizar el impacto de los riesgos si se llegaran a materializar.
23	Realizar un informe de oportunidades de mejoramiento y matriz de riesgos.

D	ACTIVIDADES PARA LA AUDITORIA DE APLICATIVOS EN DESARROLLO
1	Conocimiento del área de desarrollo de aplicaciones (personal, herramientas y cargas de trabajo)
2	Verificar la documentación sobre la funciones del área de desarrollo.
3	Verificar la existencia de un organigrama con la estructura de al área, y descripción de las funciones a desempeñar del personal.
4	Evaluar y analizar la justificación para el desarrollo del nuevo sistema de información.
5	Revisar la documentación de la evaluación costo-beneficio del programa.

6	Evaluar la visión y metas que tendrá el sistema de información.
7	Evaluar si el sistema cuenta con un objetivo
8	Analizar la metodología y levantamiento de información que se tendrá encuentra para el desarrollo del sistema. (las visiones y expectativas)
9	Evaluar el nivel de satisfacción y beneficio que tendrá el nuevo sistema de información.
10	Verificar la existencia de Modelizacion del proceso, diagramas de contexto,.
11	Analizar el diseño, interfaces del sistema de información.
12	Evaluar los requerimientos de hardware y software que requiera el sistema de información.
13	Evaluar la documentación del código fuente y código objeto.
14	Evaluar la elaboración de manuales técnicos, usuario y mantenimiento.
15	Verificación y observación de las pruebas del nuevo sistema.
16	Analizar los resultados obtenidos en el proceso.
17	Evaluar y analizar el impacto de los riesgos si se llegaran a materializar.
18	Realizar un informe de los hallazgos, recomendaciones y oportunidades de mejoramiento.

E	ACTIVIDADES PARA LA AUDITORIA FISICA
1	Conocer las instalaciones de la sede C.
2	Entrevistar al personal involucrado en el área.
3	Evaluar los controles de acceso al edificio.
4	Evaluar la seguridad de acceso a los equipos de computo.
5	Observar las edificaciones que se encuentran alrededor del centro de computo.
6	Observar y evaluar el comportamiento del servicio de los funcionarios del área.
7	Observar si existen sistemas de seguridad.
8	Evaluar los equipos de emergencia en el momento de una catástrofe (extintores, mangueras, etc.).
9	Evaluar cuantas revisiones al año se le hace a los equipos de emergencia (extintores, mangueras, etc.)
10	Verificar si al personal de la sede C, se le capacita para cuando se presenta una emergencia (simulacros).
11	Verificar y observar las rutas de evacuación.
12	Analizar y observar el reglamento y el comportamiento que se debe tener en la sede C.
13	Evaluar y analizar la estructura del edificio y medidas de seguridad.
14	Obtener información por medio de la información.
15	Analizar los resultados obtenidos en el proceso.
16	Evaluar y analizar el impacto de los riesgos si se llegaran a materializar.
17	Realizar un informe de los hallazgos, recomendaciones y oportunidades de mejoramiento.

Tabla 3.1: Actividades auditoria integral de sistemas.

F. REVISIÓN EN CUANTO AL ENFOQUE Y ALCANCE

Teniendo como conocimiento que el Área de Sistemas de la Corporación Universitaria Unitec, tiene como disposición y uso de mantener el buen funcionamiento y rendimiento de la red de la universidad, es de nuestro interés velar por la seguridad de la parte técnica y humana que allí se encuentra.

Debido a que la sede C alberga gran parte de la comunidad Uniteista, es necesario garantizar las medidas de seguridad básicas tanto de la infraestructura física como de los equipos.

ELABORÓ: Niyareth Marcela Mayorga

Oscar Javier Bautista

APROBÓ: Gustavo Adolfo Cruz

Capítulo 4
AUDITORIA DE RED

4.1 CONCEPTO AUDITORIA DE RED

Consiste en examinar detalladamente el diseño de la red, los componentes que la conforman su aprovechamiento y configuración. Se examinan las tecnologías y estándares implementados. Se aprovecha información de evaluaciones anteriores y finalmente se emiten recomendaciones que impliquen posibles mejoras en la red. Algunas de estas consistirán en cambios en software o en configuración de los equipos. Otros cambios pueden sugerir modificaciones a nivel de hardware o topología; ya sea incrementando las capacidades en los equipos actuales o agregando nuevo equipamiento. La filosofía inmersa en estas recomendaciones es siempre la de un consultor imparcial, se intentará mantener la tendencia de proveedores conocidos por el cliente o bien, la de emitir recomendaciones abiertas sin definir marcas y modelos específicos de componentes.

Dentro de una auditoria de red se procede a analizar:

- Topología
- Equipamiento
- Configuración de Servidores y nodos de usuario (desde el punto de vista de la red estrictamente. No se trata de una afinación local de cada equipo).
- Direccionamiento.
- Resolución de Nombres

- Salidas a Internet
- Estándares Utilizados.
- Errores reportados por equipos de red
- Metodología utilizada para la administración y monitoreo de la red.

4.2 COMPONENTES DE LA AUDITORIA DE RED

La arquitectura de la red se define por la visión de cada uno de los esquemas de cada parte:

Físico: Desde el punto de vista del hardware, es decir la distribución física de las máquinas y topología. Dentro de esta auditoria se deberá:

- Comprobar la existencia de áreas controladas para los equipos de comunicaciones, previendo así accesos inadecuados.
- Verificar la existencia de protección y tendido adecuado de cable y líneas de comunicaciones, para evitar accesos físicos no autorizados.
- Evaluar la existencia de controles específicos en caso de que utilicen líneas telefónicas normales con acceso a la red de datos para prevenir accesos no autorizados al sistema o a la red.

Lógico: En el que se indican qué servicios se prestan en cada máquina de la red, los tipos de tráfico, la estructura lógica de la red (divisiones en subredes, LANs, etc). Dentro de esta auditoria se deberá:

- Comprobar la existencia de contraseñas y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado a la red de comunicación.
- Verificar la existencia de facilidades de control de errores de transmisión y establecer los retransmisores apropiados.
- Evidenciar la existencia de controles adecuados que cubran la importación o exportación de datos a través de puertas en cualquier punto de la red a otros sistemas informáticos.

Administrativo: Evalúa o comprueba qué personal está encargado de cada una de las tareas relacionadas con la gestión de la red. Dentro de esta auditoria se deberá asegurar que exista una función formal de administración de la red local.

4.3 PARTICIPACIÓN DEL AUDITOR

- Evaluar que el tamaño de la red soporte el rango de coberturas inicialmente dimensionadas.
- Analizar la posible escalabilidad de los recursos informáticos.
- Analizar la tolerancia a posibles fallas de la red.
- Evaluar el nivel de rendimiento de la red.
- Evaluar la capacidad de resolución de problemas presentados en la red.
- Verificar que existan servicios de mantenimiento preventivo y correctivo en la red.

- Revisar las políticas de manejo de respaldo de información e implementación de las mismas.
- Analizar la configuración correcta de los sistemas operativos.
- Analizar la actualización de tecnología de software utilizado.
- Analizar la disponibilidad de las licencias y permisos de instalación del software en la red.
- Analizar el funcionamiento de los protocolos con detección de errores.
- Verificación de integridad de comunicación entre redes.
- Verificar políticas que restrinjan la instalación de programas o equipos en la red.
- Analizar los procedimientos de vigilancia sobre cualquier acción en la red.
- Verificar que tanto el software como el hardware sean accesados por el personal autorizado.
- Verificar que las transmisiones solo sean recibidas por el destinatario seleccionado.
- Verificar que la información sensible viaje encriptada.
- Analizar la prevención de accesos múltiples.
- Analizar la prevención de todas aquellas acciones para ingresar al sistema sin autorización correspondiente.
- Verificar el nivel de acceso a diferentes servidores en la red.
- Verificar los niveles de acceso a los diferentes servicios brindados en la red.

- Verificar la implementación de nuevos servicios según la capacidad de la red y las necesidades de los usuarios.
- Analizar los procedimientos de protección de los cables y la toma de conexión.
- Verificar las medidas de seguridad para la protección de las diferentes líneas según su especialización (voz y data).
- Analizar el diseño arquitectónico de las instalaciones de la red.
- Verificar que existen adecuados procedimientos de aprobación de presupuestos sobre la gestión de la red.
- Comprobar que la gerencia de comunicaciones posea cierto grado de decisión que permita la mejor gestión administrativa y tecnológica.

4.4 CUESTIONARIOS QUE SE APLICAN EN UNA AUDITORIA DE RED

4.4.1 CUESTIOINARIO PARA ADMINISTRADOR DE RED PRINCIPAL

TEMA: AUDITORIA DE RED PARTE LOGICA Y FISICA

FECHA: 25/05/2005

NOMBRE DEL ENTREVISTADO:

CARGO:

Verificar de que existan contraseñas y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado a la red.

Códigos de control

- **Contraseñas**

Comentarios:

- Analizar la asignación y control de contraseñas.
- Documentar con respecto a la historia los cambios de contraseña.
- Tomar nota del método en que podría burlarse las contraseñas.
- Examinar la técnica de control para verificar su eficacia.
- Describir los niveles de contraseña.

1. ¿Para acceder a cada uno de los servidores de la red utilizan ustedes la misma contraseña.?
2. ¿Que tipo de contraseña utilizan?
   - Contraseña dada por el Administrador. ( )
   - Contraseñas al azar dadas por el sistema. ( )
   - Códigos de acceso generados al azar por el sistema. ( )
   - Frases de acceso. ( )
   - Secuencias de preguntas y respuestas interactivos. ( )
   - Predeterminadas por coordinadas generadas por código. ( )
3. ¿Hay en practica un procedimiento adecuado de control de las contraseñas para proteger la utilización del sistema?.
4. ¿Se utiliza un sistema de contraseñas orientado a los usuarios?.
5. ¿Es efectivo el control el control sobre la expedición y uso de las contraseñas?.

6. ¿Se cambia y vuelven a expedir todas las contraseñas por lo menos dos veces al año, y son desactivadas inmediatamente después que el titular es despedido o desautorizado? .
7. ¿se dispone de procedimientos según los cuales un usuario puede hacer invalidar inmediatamente su contraseña y lograr que se le expida una nueva cuando crea que se ha violado la suya?.
8. ¿Están eficazmente restringidos los procedimientos parta burlar el sistema de control de contraseñas?.
9. ¿Se define en los procedimientos que describen el sistema de control de contraseñas, las condiciones especiales que se necesitan para burlarlas?
10. ¿Esta diseñado el sistema de contraseñas de modo que prohíba a ciertos usuarios y/o sitios el acceso a ciertos datos?.
11. ¿ Son las contraseñas lo suficientemente largas para tener suficientes combinaciones de modo que no pueda violarse fácilmente?.

CODIGOS DE SEGURIDAD Y AUTORIZACIÓN

Comentarios:

- Incluir una definición del procedimiento de control en los papeles de trabajo.
- Describir la estructura de los códigos y sus atributos.
- Identificar a personas que, en caso de confabulación podrían burlar los controles de expedición.

12. ¿utiliza un código de seguridad además de las contraseñas?.
13. ¿Quién asigna los códigos de seguridad?

14. ¿Es eficaz el control de la expedición y la utilización de los códigos de seguridad?.
15. ¿Se ejerce control sobre la autorización de los usuarios?.
16. ¿Esta el código de autorización estructurado de manera que permita al usuario desempeñar únicamente una función (por ejemplo, leer o actualizar)?.
17. ¿Esta el sistema de autorización de usuarios diseñado de tal modo que proteja y asegure la información de los archivos basándose en elementos de información?.
18. ¿Es eficaz el control sobre la expedición y utilización de los códigos de autorización?.

CLAVES

Comentarios:

- Definir o identificar a las personas encargadas del control de las claves.

19. ¿Se observa un procedimiento adecuado de control para proteger el uso de los archivos de datos del sistema?.
20. ¿Se utilizan claves para proteger los archivos?.
21. ¿Se aplican y controlan las claves en un lugar centralizado?.

TABLAS DE SEGURIDAD

Comentarios:

- Elaborar una lista de todas las personas que puedan iniciar, y de todas las personas que puedan implantar cambios en las tablas de seguridad.

22. ¿Se llevan controles adecuados de los sistemas de codificación de contraseña, códigos de autorización, códigos de seguridad y claves?
23. ¿Cuentan ustedes con tablas de seguridad?
24. ¿Se encarga a personal distinto del procesamiento de datos del mantenimiento de las tablas de seguridad?
25. ¿Se ejercen controles eficaces sobre los procedimientos de acceso, actualización e informes relativos al mantenimiento de las tablas internas de seguridad?.
26. ¿Realizan pruebas de comprobación de las tablas de seguridad, sacados mediante un balance interno, después de cada actualización y antes de reanudar un procedimiento?.

GARANTIZAR QUE EN UNA TRANSMISIÓN, ESTA SOLO SEA RECIBIDA POR EL DESTINATARIO.

TRANMISION DE DATOS

27. ¿Son adecuadas las prácticas de control de transmisión de datos?
28. ¿Se han establecido y documentado las convenciones de control de transmisión de datos y se usan?
29. ¿Se emplean los controles indicados a continuación para determinar la exactitud, totalidad de la transmisión?
    - ¿conteos de mensajes?
    - ¿Conteos de caracteres?
    - ¿Transmisión doble?

- ¿Líneas Condicionales?

VERIFICAR SI EXISTEN PROTOCOLOS DE CONTROL DE ERRORES DE TRASMISIÓN Y QUE HA SU VEZ DETECTEN ERRORES

30. ¿Manejan algún tipo de protocolo de control de errores de transmisión?
31. ¿Se tienen estadísticas de las tasas de errores y retransmisión?
32. ¿El bloqueo de una terminal enciende una señal de alerta?
33. ¿El desbloqueo de una terminal lo ejecuta o aprueba un supervisor? Indique el procedimiento.?

OBSERVAR Y VERIFICAR QUE PROCEDIMIENTOS SE UTILIZAN PARA QUE SE REGISTREN LAS ACTIVIDADES DE LOS USUARIOS DE LA RED DETECTANDO ASI ACCESOS NO AUTORIZADOS.

34. ¿Manejan algún mecanismo de control (software, hardware, etc) para la detección de las actividades de los usuarios? Indique el mecanismo y el funcionamiento de este o estos dentro de la red.
35. ¿El mecanismo de control es independiente o comparten un mismo recurso?.
36. ¿En caso de un acceso no autorizado que medidas de control se toman automáticamente?.
37. ¿Qué procedimientos o controles realizan, para el bloqueo de paginas web no autorizadas dentro de la red (musicales, pornográficas, etc) ?.
38. ¿Existe documentación de las licencias?
39. ¿Controlan las licencias de los anti-virus? Cual es el procedimiento.

VERIFICAR SI EXISTE NORMAS Y POLÍTICAS PARA QUE NO EXISTA LA INSTALACIÓN DE HARDWARE Y SOFTWARE ILEGAL

40.¿Cómo se controla la instalación de hardware y software ilegal, no autorizado dentro de las políticas de la red? Indicar procedimientos.

41. ¿Cómo se restringe la instalación de software ilegal?

VERIFICAR SI EXISTEN TÉCNICAS DE CIFRADO DE DATOS PARA QUE NO HAYA RIESGO DE ACCESOS IMPROPIOS A TRASMISIONES SENSIBLES CRIPTOGRAFIA Y DATOS

42. ¿Se utilizan niveles adecuados de cifrado?

43. ¿Es el programa de cifrado lo suficientemente complejo como para que una persona que posea la clave pero no el programa, no pueda hacer uso de éste?

44. ¿Se dispone de procedimientos de seguridad externa que impidan que una persona tenga acceso tanto a la clave como al programa?

TRANSMISIÓN DE DATOS SENSITIVOS

45.¿Hay en efecto procedimientos especiales de manejo para asegurar que los datos sensitivos no pueden ser transmitidos inadvertidamente a otro terminal de red?

OBSERVAR SI LA PROPIA EMPRESA GENERA PROPIOS ATAQUE S PARA PROBAR SOLIDEZ DE LA RED Y ENCONTRAR POSIBLES FALLAS

IDENTIFICACION DEL PERSONAL

46. ¿Se utiliza una técnica adecuada de identificación del personal para limitar el uso no autorizado de las terminales?.

47. ¿Se usa algún tipo de identificación dactilar o biométrica para controlar el acceso a las terminas o cuarto de maquinas?

48. ¿Se usan tarjetas de identificación para validar la autorización de acceso y uso de las terminales?

PROTECCION DE DATOS

49. ¿Se restringe el acceso para consultas y/o actualizaciones de los datos de producción a los usuarios de la red de tiempo compartido?.

50. ¿Se restringe el acceso para consultas y/o actualizaciones de los datos de otros usuarios o proyectos que se encuentren en la red de tiempo compartido?.

51. ¿Reportan los datos usados por códigos de identificación de los usuarios?

4.4.2 CUESTIONARIO PARA JEFE DEPARTAMENTO DE SISTEMAS

TEMA: AUDITORIA DE RED PARTE ADMINISTRATIVA

FECHA: 25/05/2005

NOMBRE DEL ENTREVISTADO:

CARGO:

1. ¿Son adecuados los procedimientos administrativos para los usuarios de contraseñas?

2. ¿Están documentados los procedimientos administrativos para el mantenimiento de contraseñas?

3. ¿Se hacen por escrito los requerimientos y cambios de los usuarios de la red?

4. ¿Existen Manuales de las funciones como administrador? Si no existen manuales como se comunican las funciones al personal de sistema.

5. ¿En caso de emergencia, que el administrador se retire por vacaciones o despido, existe alguna persona capacitada para reemplazarlo?

6. ¿cómo garantizan de que se este utilizando la mejor tecnología para beneficio de la red?

7. ¿se realizan procedimientos de control y seguridad a la red?

8. ¿cómo Jefe de Departamento programa capacitación a los usuarios de la red?

Capítulo 5
AUDITORIA APLICATIVOS EN DESARROLLO

5.1 CONCEPTO AUDITORIA APLICATIVOS EN DESARROLLO

Es la evaluación de la existencia y aplicación de procedimientos de control adecuados que permitan garantizar que el desarrollo de sistemas de información se ha llevado a cabo.

Abarca todas las fases que se deben seguir desde que aparece la necesidad de disponer de un determinado sistema de información hasta que es construido e implantado. [1]

Incluye todo el ciclo de vida del software excepto el mantenimiento y la retirada del servicio de las aplicaciones cuando esta tenga lugar.

La Auditoria a Aplicativos en Desarrollo debe considerar entre otras las siguientes actividades:

1.- Estudio de Viabilidad de la Aplicación. Es muy importante para los casos de Aplicaciones largas, complejas y de alto costo.

2.- Definición Lógica de la Aplicación. Se analizará que se hayan implementado postulados lógicos, en función de la metodología elegida y la finalidad que persigue el proyecto.

[1] http://www.auditnet.org/ (28 de Marzo de 2005)

3.- Desarrollo Técnico de la Aplicación. Se verificará que cumpla una secuencia ordenada de pasos y una metodología funcional. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles.

4.- Diseño de Programas. Deberán poseer la máxima modularidad, sencillez y economía de recursos.

5.- Métodos de Prueba. Se realizarán de acuerdo a las Normas de Instalación.

Se utilizarán datos de prueba, sin que sea permisible el uso de datos reales.

Cuando existan ambientes de trabajo diferenciados, se realizarán pruebas; sólo cuando éstas hayan terminado con éxito, se realizarán pruebas finales en producción.

6.- Documentación. Cumplirá la Normativa establecida en la Instalación, tanto la técnica como la de usuario final.

7.- Equipo de Programación. Deben fijarse las tareas de análisis puro, de programación, y las intermedias. En Aplicaciones complejas, se producirán variaciones en la composición del grupo, pero éstas deberán estar previstas.

La coordinación de actividades corresponde al Jefe del Proyecto, el cual reporta al responsable del Área de Desarrollo.

Esta auditoria incluye también el análisis y observación de satisfacción de usuarios verificando que se cuente con sus puntos de vista y la presencia de este para proporcionar grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

5.2 PARTICIPACIÓN DEL AUDITOR

Aún cuando el auditor esté interesado en todos los aspectos del nuevo sistema, debe velar porque se establezcan todos los controles de aplicación. Su principal función es asegurar que los sistemas, recientemente implantados incluyan características de control sólidas y confiables. En términos generales es ayudar a prevenir que se implanten sistemas de aplicación que tengan riesgos de alto impacto. El auditor participa en el proceso de desarrollo de sistemas evaluando la documentación generada como producto final de las primeras fases del ciclo de vida del sistema.

En estas actividades su interés se concentrará primordialmente en el desarrollo e implantación de controles de aplicación adecuados. El auditor necesita reconocer que su participación durante el desarrollo de los sistemas puede amenazar su independencia y deberá tomar medidas para evitar esta pérdida.

Estas medidas incluyen:

- Permanecer organizacionalmente independiente del grupo de sistema. Esto significa que el auditor no es un miembro en propiedad del grupo de desarrollo de sistema y no le quita la dirección del proyecto al gerente del grupo del proyecto.
- Redactar los informes independientemente del grupo del proyecto. Las opiniones del auditor, sus recomendaciones y sus evaluaciones no deberían incluirse en los informes de status del proyecto puesto que el

emisor de los informes (usualmente el gerente del grupo del proyecto) tiene autoridad editorial para modificar las observaciones del auditor.

- Investigar independientemente al equipo del proyecto. Con este puede estar restringido a ciertos contactos y cierta autoridad, pero el auditor tiene libre acceso a la información y al personal de la organización.

5.3 CUESTIONARIOS QUE SE APLICAN EN UNA AUDITORIA DE APLICATIVOS EN DESARROLLO

5.3.1 CUESTIONARIO PARA ANALISTAS Y PROGRAMADORES

TEMA: AUDITORIA APLICATIVOS EN DESARROLLO

FECHA: 25/05/2005

NOMBRE DEL ENTREVISTADO:

CARGO:

FASE DE PLANEACION

- **Necesidad**

1. ¿Cómo surgió la necesidad?
2. ¿Por qué personas fue iniciada la solicitud?
3. ¿Cómo fue el proceso de solicitud por parte del usuario a los analistas?
4. ¿ Cómo se hizo el proceso de aprobación?

- **Problema**

5. ¿Lleva un cronograma de actividades para el proyecto? ¿Cómo tiene programadas las fases? ¿Qué tiempo toma la elaboración del proyecto?

6. ¿Existe documentación sobre la descripción del problema y justificación de este proyecto? (CONOCIMIENTO)

7. ¿Se cuenta con un estudio y documentación del sistema actual con todas sus debilidades y fortalezas del sistema?

8. ¿Se han hecho debidamente las delimitaciones del proyecto (espacial, cronológica, financiera, conceptual)?¿Quién es el encargado de hacer este estudio?

9. ¿Se exigió que el usuario asignara un representante para que participe en el desarrollo del proyecto?

10. ¿El departamento de sistemas asigno algún gerente líder del proyecto?

11.¿El proyecto esta clasificado en mayor, mediano o menor de acuerdo a su costo estimado de desarrollo? ¿Cual?

12. ¿El gerente del proyecto prepara recomendaciones y se asegura que estas sean aprobadas por el usuario?

13. ¿Existe Documentación que describa el sistema actual y se ha realizado un diagnostico que especifique Tareas y errores?

- **Etapa de Definición**

14. ¿Se definió y se estableció el tipo de Hw, Sw, redes que posee el área o empresa en la para la implementación del software?

15¿Se describe brevemente cada área del organigrama, sistemas operativos y equipos para el estudio de un nuevo sistema?

16 ¿Se tiene conocimiento general del área en la que se implementara el proyecto (personas que conforman el organigrama, misión, visión, principios filosóficos etc.)?

FASE DE ANÁLISIS

17¿Cuáles fueron los métodos de levantamiento de información que se implementaron (entrevistas, encuestas, cuestionarios, reuniones etc.)?

- **Levantamiento de Información**

18. ¿Se tiene estructuración de encuestas?

19. ¿Se realizo el estudio de población a la que se le aplica las encuestas?

20. ¿De acuerdo con el levantamiento de información se obtuvieron estadísticas(tabulación de encuestas y graficas) del problema, y se observo totalmente el funcionamiento y estado del sistema actual?

- **Observación, Análisis y Resultado**

21. ¿Se indican por escritos las diferentes alternativas y soluciones que se le dieron al sistema actual dando a reconocer recursos (humanos, físicos (hardware y software) y financieros) e incluyendo ventajes y desventajas que ofrecía este?

22. ¿Existe evaluación de alternativas, se deja evidencia de las evaluaciones

23. Se toman decisiones con los resultados de la evaluación de alternativas?

FASE DE DISEÑO

24. ¿Dentro de las políticas del sistema propuesto final se han llevado a cabo la modelización de procesos y diagramas de contexto?

25. ¿Se lleva acabo un Modelo (representación grafica de un sistema que puede modificarse y adecuarse para alcanzar los objetivos propuestos)? ¿Cuál de las Siguientes utiliza?

- Modelo Secuencial Lineal (cascada) - Constituido por análisis, diseño, codificación, pruebas, mantenimiento. Los errores pueden verse al final del análisis.
- Modelo de Construcción de Prototipos – Se toman los requerimientos de usuario mientras el ingeniero hace el levantamiento de información y entrega un diseño pequeño.
- Modelo de Desarrollo Rápido – Se establecen requisitos y se debe limitar al ámbito del proyecto y utiliza tres fases. (Modelo de procesos, Modelado de datos, Modelo de gestión)

26. ¿Se utilizan mecanismos para gestión y desarrollo del proyecto (Modelizacion de datos(Técnica para la organización y documentación de los datos de un sistema), Diagramas Entidad Relación (Bases de datos, categorización de datos

dentro del sistema), Modelizacion de redes (Para describir la forma del sistema de información))?

27. Se utilizan mecanismos para gestión y desarrollo del proyecto como:

- Modelizacion de Datos - Forma en la que se va a llevar la información, organización y documentación de datos del sistema. Se lleva a cabo el diagrama entidad.-relación (Categorización de datos dentro del sistema
- Modelizacion de Redes – Se emplean diagramas para describir la forma del sistema de información para tener en cuenta necesidades de red, puestos esenciales y poder llevar un conocimiento acerca de cómo se llevara la conectividad de los módulos del SIG.

28. Se llevan a cabo las especificaciones y características técnicas de equipos en el área?

29. ¿Quiénes participan en la elección del diseño?

30. ¿Cómo se colocan de acuerdo para esta elección?

31. Se tiene productos tangibles de:

- Propuesta del diseño
- Revisión del diseño
- Presentación a la gerencia
- Propuesta de gastos mayores

32. ¿Se tienen en cuenta y actualmente se esta trabajando en la documentación de los programas, manual de usuario, manual de operación-producción, documentación de la prueba de aceptación y presentación a la gerencia?

33. ¿Se lleva acabo un plano de interfaz final de usuario?

34. ¿Se lleva acabo un plano funcional del sistema?

FASE DE CONSTRUCCIÓN

35. ¿Se ha hecho una codificación basada en las etapas anteriores?

36. ¿Se han realizado pruebas de funcionamiento del programa y se tiene documentación de estas pruebas?

37. ¿Cómo Se ha llevado a cabo la implantación del software?

SOPORTE

38.¿Se ha hecho seguimiento al software para observa si esta cumpliendo con sus tareas?¿Cómo llevan acabo este seguimiento?

Capítulo 6
AUDITORIA FÍSICA

6.1 CONCEPTO DE AUDITORIA FÍSICA

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.

Entre las precauciones que se deben revisar están:

- Contar con detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de los laboratorios.
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- Se debe verificar que existan suficientes salidas de emergencia y que estén
- Debidamente controladas para evitar robos por medio de estas salidas.

6.2 PARTICIPACION DEL AUDITOR

En la auditoria a la seguridad física, se evaluara la confiabilidad física a:

- Datos.
- Instalaciones.
- Equipos.
- Redes y soportes.

En este tipo de auditorias se controlan, por ejemplo: control de accesos, identificación, instalaciones, servidores, medios y procesos de almacenamiento, etc.

También se tiene como principal consideración velar por la seguridad humana, lo cual requiere que se encuentren protegidas y existan medidas de evacuación, alarmas para así poder evitar que el personal se encuentre expuesto a riesgos superiores considerados por la empresa e incluso en el sector o área de trabajo.

En una Auditoria de sistemas de información, nos preocupamos especialmente por quienes están en el área o de los daños que puedan afectar a los usuarios de los sistemas.

Las amenazas pueden ser muy diversas:

- Sabotaje.
- Vandalismo.
- Terrorismo.
- Accidentes de distinto tipo.
- Incendios.
- Inundaciones.
- Averías.
- Derrumbamientos.
- Explosiones.

Así como otros que afecten la integridad de las personas y puedan interrumpir el funcionamiento de los centros de cómputo tales como:

- Errores.
- Negligencias.
- Huelgas.
- Epidemias
- Intoxicaciones.

Desde una perspectiva de seguridad física podemos considerar algunos aspectos como:

- Ubicación del centro de procesos, los servidores y en general cualquier elemento a proteger, como pueden ser las propias terminales, especialmente en zonas de mayor circulación por el personal que allí se encuentre trabajando, acceso publico, o cercanos a ventanas que llegasen a estar en contacto al exterior del centro de computo.
- También se tendrá en cuenta la estructura, diseño, construcción y distribución de los edificios.
- Riesgos a los que estén expuestos, ya sea por agentes externos, o por accesos físicos no controlados.
- Amenazas de fuego (materiales empleados); riesgos por agua: por accidentes atmosféricos o por averías en las tuberías; problemas en el suministro eléctrico, tanto por caídas como perturbaciones.
- Además del control de acceso, en determinados edificios o áreas debe controlarse el contenido de carteras, paquetes, bolsos o cajas, ya que podrían tener explosivos, así como lo que se pudiese sacar del edificio, para poder evitar sustituciones en los equipos, componentes, soportes magnéticos, documentación u otra clase de archivos. El control de revisión deberá afectar a las visitas, proveedores, contratados, clientes y en casos

mas estrictos igualmente a los empleados. Los ex empleados deberán considerarse como visitas.

- La protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte, además de otras protecciones no físicas, todo bajo un sistema de inventario, así como documentos que se encuentren impresos y de cualquier tipo de documentación clasificada. Igualmente es fácil y barato tener copias magnéticas las cuales se realicen periódicamente.

6.3 CUESTIONARIOS QUE SE APLICAN EN UNA AUDITORIA FÍSICA

6.3.1 CUESTIONARIO PARA ADMINISTRADOR DE SALAS DE INFORMATICA

TEMA: AUDITORIA SEGURIDAD FISICA SEDE C

FECHA: 25/05/2005

NOMBRE DEL ENTREVISTADO:

CARGO:

1. Nombre y cargo que desempeña en UNITEC.
2. Horario en que trabaja en UNITEC.
3. ¿Existe un grupo de trabajo?, ¿Cuántos?, ¿Qué desempeñan en la sede?
4. En promedio, cuántos alumnos ingresan a la sede C durante su periodo de trabajo.

5. Con cuántos equipos de computo cuenta la sede C.
6. ¿Existen una persona responsable de la seguridad?
7. ¿Cómo se controla el acceso y el uso de las salas de computo?
8. ¿Tiene el cuarto de máquinas una instalación de escaparate y, si es así, pueden ser rotos los vidrios con facilidad?
9. ¿Cuáles son los sistemas de control de acceso físico a la sede C?
10. ¿Son controladas las visitas y demostraciones en el centro de cómputo? ¿Cómo son controladas?
11. ¿Cuántas copias de llaves existen de cada una de las salas que alberga la sede C, y como están distribuidas?
12. ¿Dónde está ubicado el centro eléctrico (tacos)?
13. ¿Cuántas personas tienen acceso (autorizado) al centro eléctrico? ¿Quiénes son?
14. ¿Cuántas entradas (acometidas) de luz posee la sede C?
15. La sede C, ¿posee equipos eléctricos de respaldo y dónde están ubicados y cuanto tiempo de servicio prestan?
16. ¿La sede posee salidas de emergencia?
17. Existe alarma para:
    - Detectar fuego /calor o humo) en forma automática?
    - Avisar en forma manual la presencia del fuego?
    - Detectar una fuga de agua?

- Detectar magnetos?
- No existe?

18. Estas alarmas están en las salas de computo y pasillos de la sede C.
19. ¿Existe alarma para detectar condiciones anormales del ambiente?
20. ¿La alarma es perfectamente audible?
21. ¿Esta alarma también está conectada?
    - Al puesto de guardias?
    - A la estación de bomberos?
    - A ningún otro lado?
    - Otro
22. ¿Existe un plan de distribución de los extintores en la sede C?
23. Existen extintores de fuego?
    - Manuales?
    - Automáticos?
    - No existen?
24. ¿Se ha adiestrado el personal en el manejo de los extintores?
25. ¿Los extintores, manuales o automáticos a base de
    - Agua
    - Gas
    - Otros
26. ¿Los alumnos saben que hacer en caso de una emergencia?

27. ¿Existe salida de emergencia?
28. ¿Se ha capacitado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
29. ¿Se ha prohibido a los usuarios el consumo de alimentos y bebidas en el interior del cuarto de máquinas para evitar daños al equipo?
30. ¿Se limpia con frecuencia el polvo acumulado dentro de las salas?
31. ¿Tiene usted conocimiento de los planes de contingencia contemplados para la sede C?
32. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
33. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.
34. ¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
35. ¿Tienen seguros todos estos equipos?

6.3.2 CUESTIONARIO PARA JEFE DE SEGURIDAD Y DE COMPRAS

TEMA: AUDITORIA SEGURIDAD FISICA SEDE C
FECHA: 25/05/2005
NOMBRE DEL ENTREVISTADO:
CARGO:

1. Nombre y Cargo que desempeña en UNITEC.

2. Horario de trabajo en UNITEC.
3. ¿Cuánto tiempo de construido tiene la edificación de la sede C?
4. ¿Qué funcionaba allí antes de ser adquirido por UNITEC?
5. ¿Cuándo fue adquirida la edificación por UNITEC?
6. En el momento de comprarlo ¿UNITEC realizó estudios a la edificación para determinar su estado, (sismos, suelos, desagües, flujo eléctrico, etc.)?
7. ¿El edificio sufrió alguna adecuación para ser usado por UNITEC? ¿Cuál?
8. ¿Quién realizó la adecuación de las instalaciones del edificio?
9. ¿Durante el proceso de adecuación, existió un proceso de auditoria? ¿Quién lo realizó?
10. ¿Existe algún seguro contratado para la sede C? ¿Qué cubre?
11. Actualmente, ¿la universidad cuenta con un plan de contingencia sobre la sede C? ¿Qué riesgos contemplan y que medidas consagra?
12. El personal de la sede C, se encuentra capacitado para cualquier eventualidad como incendios, etc.
13. ¿Existe personal de vigilancia en la institución?
14. La vigilancia se contrata, directamente o por medio de empresas que presten este servicio.
15. El edificio donde se encuentra la computadora esta situado a salvo de:
    a) Inundación?
    b) Terremoto?

c) Fuego?

d) Sabotaje?

16. Existe un plan de distribución de los extintores en la sede C?
17. Existen extintores de fuego?
    - Manuales
    - Automáticos ¿ Si son automáticos son encendidos por los detectores de fuego
    - No existen?
18. ¿ Los extintores apagan todo tipo de fuego causado por químicos, plástico, cortos circuitos, etc.?
19. ¿Se ha capacitado el personal en el manejo de los extintores?
20. ¿Se revisa dé acuerdo con el proveedor el funcionamiento de los extintores?

6.3.3 CUESTIONARIO PARA COORDINADOR DE SEGURIDAD

TEMA: AUDITORIA SEGURIDAD FISICA SEDE C
FECHA: 25/05/2005
NOMBRE DEL ENTREVISTADO:
CARGO:

1. Nombre y cargo que desempeña en Unitec.
2. ¿Usted es la persona responsable de la seguridad?

3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
4. ¿La vigilancia se contrata, directamente por la universidad o por medio de una empresa que preste este servicio?
5. ¿Se investiga a los vigilantes cuando son contratados directamente?
6. ¿En cuanto a la sede C, usted tiene conocimiento de la seguridad que allí hay?
7. Existe alarma para:
    - Detectar fuego /calor o humo) en forma automática?
    - Avisar en forma manual la presencia del fuego?
    - Detectar una fuga de agua?
    - Detectar magnetos?
    - No existe
8. ¿Estas alarmas avisan en forma manual la presencia de fuego?.
9. ¿Existe alarma para detectar condiciones anormales del ambiente?
10. ¿La alarma es perfectamente audible?
11. ¿Estas alarmas tienen algún control, en los puestos de guardias?
12. ¿Esta alarma también está conectada?

- Al puesto de guardias?
- A la estación de bomberos?
- A ningún otro lado?

- Otro

13. ¿Existe un plan de distribución de los extintores en la sede C?
14. Existen extintores de fuego?
    - Manuales
    - Automáticos
    - No existen?

15. ¿ Los extintores apagan todo tipo de fuego causado por químicos, plástico, cortos circuitos, etc.?
16. ¿Se ha capacitado el personal en el manejo de los extintores?
17. ¿Saben qué hacer los operadores del cuarto de máquinas en caso de que ocurra una emergencia ocasionada por fuego?
18. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?
19. ¿Se revisa dé acuerdo con el proveedor el funcionamiento de los extintores?
20. ¿Cuántos accesos tiene la sede C?
21. ¿Cómo se maneja la rotación del personal de seguridad?
22. Aparte del personal ¿Con qué otros sistemas de seguridad y vigilancia cuenta la sede C?
23. ¿Cambia las medidas de seguridad en las horas nocturnas?

24. ¿Quién es el encargado de activar los sistemas de seguridad (alarmas, censores, etc.)?
25. ¿UNITEC, cuenta con sistemas externos de seguridad?
26. ¿Cómo se realiza el control de acceso a la sede C? ¿Existen limitaciones (horarios)?
27. ¿Existe una comunicación directa con la policía?
28. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?

Capítulo 7
ANÁLISIS DE RESULTADOS

7.1 AUDITORIA DE RED

7.1.1 INTRODUCCIÓN

Durante el período comprendido entre Febrero 5 y Abril 3 de 2005, se llevó a cabo un proceso de auditoria a la CORPORACIÓN UNIVERSITARIA UNITEC, donde se evalúo la parte física, lógica y administrativa de red.

Se utilizaron métodos de levantamiento de información como las entrevistas, observación y fotografías a la red.

Así mismo, se presenta todo el procedimiento que se realizó y un informe final en el que se consignan los diferentes hallazgos, observaciones y obviamente las recomendaciones que el equipo auditor aporta para optimizar el funcionamiento y distribución de la red.

7.1.2 INFORME FINAL DE AUDITORIA DE RED

CORPORACION UNIVERSITARIA UNITEC
AUDITORIA INTEGRAL DE SISTEMAS
EVALUACION DE RED

I. OBJETIVO

Evaluar las condiciones físicas, lógicas y administrativas de la red, determinando, el cumplimiento de políticas, normas y procedimientos establecidos por la institución.

II. ALCANCE

Atendiendo normas de auditoria generalmente aceptadas y de acuerdo con el sistema de control interno informático implementado por Unitec, valoramos los subprocesos físicos, lógicos y administrativos de la red corporativa.

Efectuamos el análisis entre el 5 de febrero y el 3 de Abril del 2005.

III. OPORTUNIDADES DE MEJORAMIETO

1. Modificación de contraseñas en los laboratorios de informática

Establecimos que las contraseñas que se manejan en los laboratorios de informática con el perfil de administrador, carecen de estándares que se deben tener en cuenta en el momento de su creación.

Existe el riesgo que puedan ser observadas y memorizadas por los usuarios al ser digitadas por el administrador.

Por lo tanto recomendamos que las contraseñas sean mínimo de ocho caracteres, que incluyan mayúsculas, minúsculas, números y símbolos.

2. Organización de cableado

Se observó, en la sede A, canaletas con cables sueltos y a la vista, facilitando la conexión no autorizada de equipos portátiles a la red. **(Ver Anexo No AIR-001)**

Se recomienda suprimir estos cables si no esta prestando servicio en la red.

3. Identificación del Cableado

El cableado de las sedes B, E, G, F no se encuentra debidamente etiquetado ni Codificado. **(Ver Anexo No AIR-002)**

En este caso se corre el riesgo que los patch cord sean desconectados del switch o Patch panel y al conectar nuevamente se presenten problemas de funcionamiento y organización.

Se recomienda tener un etiquetado y a la vez una documentación del sistema de cableado instalado, en cada una de las sedes por lo cual se sugiere seguir la norma ANSI TIA/EIA 606. que garantiza una mejor administración de la red, y crear un método de seguimiento ya sea para traslados, cambios, adiciones facilitando la localización de fallas.

Se recomienda también verificar la identificación del cableado (C), closet de telecomunicaciones (TC), Áreas de trabajo (WA), en las sedes anteriormente nombradas.

Para cumplir esta norma se debe tener en cuenta la existencia de planos para ilustrar etapas diferentes de implementación e instalación ya sea conceptual o gráfica.

De igual forma se recomienda elaborar, en un software (Autocad), la ilustración grafica que especifique todos los ductos, elementos y rutas con una convención clara para el lector.

También se de debe tener en cuenta:

- Listar tanto al personal responsable de las operaciones físicas, como a aquellos responsables de actualizar la documentación.
- Se recomienda etiquetar y listar todas las rutas y espacios a través de adhesivos o técnicas de inserción.

4. Reubicación de Switch

Evidenciamos que los Armarios, Racks y Switch carecen de una ubicación y climatización, en cada una de las Sedes de Unitec.

A continuación damos a conocer una tabla generalizada de la ubicación de las terminales en cada una de las sedes:

SEDE	PROBLEMA	RECOMENDACION
A	Observamos que los armarios que resguardan los switch, routers, módems carecen, de seguridad. (Ver Anexo No AIR-003) se evidencio que son de fácil acceso y junto a ellos se encuentran las llaves, y las puertas abiertas. (Ver Anexo No AIR-003)	Recomendamos que las llaves sean guardadas en sitio remoto bajo la custodia del administrador.
B.	Evidenciamos que el Switch se encuentra situado en una esquina sobre el piso, acompañado de elementos como camisetas, trofeos, banderas, etc. (Ver Anexo No AIR-004) Este cuarto carece de condiciones adecuadas para el funcionamiento del Switch, corriéndose el riesgo que los cables sean desconectados o pisados,	Se recomienda que el Switch este por lo menos a un metro del piso, dentro de una caja metálica y el cableado este debidamente etiquetado y sin elementos alrededor de él.

	afectar la continuidad de las operaciones. Adicionalmente el cableado esta sin codificación ni etiquetado.	
E.	A través del estudio que se realizó en esta Sede, observamos que el Rack y el servidor se encuentran sobre el suelo, también se evidenció falta de organización del cableado en los Switch, no se cuenta con iluminación ni control de temperatura, el piso se encuentra alfombrado. (Ver Anexo No AIR-005)	Se recomienda la Reubicación de los componentes en un cuarto más amplio, mantener la parte eléctrica separada de la parte de datos e implementar controles de climatización, organización y etiquetado del cableado. Otra alternativa seria que los switch, Modems, etc. Se resguardaran dentro de un armario con seguridad y climatización para estos componentes.
F.	Apreciamos que el Rack se encuentra dentro de la misma sala del administrador, encima de una mesa auxiliar de escritorio, no existe organización ni etiquetada de cableado y el servidor DHCP se encuentra en el piso. (Ver Anexo No AIR-006) Existe el riesgo de que el Rack se caiga de la mesa o que sean desconectados los cables del Switch o Patch Panel ya que se encuentran a la mano de cualquier persona. De igual manera se observo que el piso de la sala es en caucho e inflamable y dentro de esta sede no se cuenta con una fuente eléctrica de respaldo para los equipos.	Es necesario disponer de un cuarto o armario apropiado para los componentes (Switch, servidor, módem, VPN etc) teniendo en cuenta condiciones ambientales, etiquetado y codificación de cableado.
G.	Observamos deficiencias en el estado de limpieza, organización y ambiente presentando problemas de humedad y suciedad que podrían afectar al Switch e interrumpir las actividades informáticas de la sede. (Ver Anexo No AIR-007)	Se recomienda remodelación, organización y limpieza a este cuarto y poner en funcionamiento el ventilador que se encuentra allí, para estabilizar la temperatura de este y así tener un lugar propicio para los componentes.

Tabla 7.1: Identificación de riesgos detallada por sedes.

5. Adecuación de Closet de Telecomunicaciones

En las sedes A, B, E, G, F se carece de instalaciones adecuadas para los medios de telecomunicaciones (Switch, servidores, módems etc.) y los cuartos donde se encuentran situados estos componentes están desprovistos de control, seguridad y temperatura, entre otros. **(Ver Anexo No AIR-008)**

Establecimos inobservancia a la norma ANSI TIA/EIA-509 respecto a el edificio debe ser adaptable a cambios por configuración y/o expansión de la red, contar con Rutas de cableado Horizontal (Ductos bajo el piso, Piso Falso, Charolas para el Cable, Rutas de techo Falso), Rutas de cableado Vertical (en rutas intra e inter edificios), Closet de Telecomunicaciones, Cuarto de equipos, Entrada de Servidores, etc.

6. Implementación de un Reglamento del administrador.

Establecimos, mediante el proceso de recolección de información, ausencia de un documento formal completo que contenga todas las funciones que debe realizar el administrador de la Red de la Corporación Universitaria Unitec.

(Ver Anexo No AIR-009)

Por lo tanto recomendamos que se estipulen parámetros de las funciones del administrador y este pueda dedicarse a su trabajo, para que no le dedique tiempo a trabajos que no le correspondan.

7. Documentación Técnica del cableado de la red.

Evidenciamos ausencia de documentos formales del cableado de la red en (Sede A, B, E, F, G). **(Ver Anexo No AIR-010)**

Se recomienda tener documentación actualizada en el diseño y cableado de la red para lograr un fácil entendimiento por parte del administrador y otras personas que llegasen a intervenir en los procesos de la red.

8. Mapa de Red

De acuerdo con el suministro de información por parte del departamento de informática, establecimos que hace falta orientar y delimitar los componentes tecnológicos que se encuentran en cada una de las Sedes de la Universidad; Dentro del mapa se deberá especificar la conexión de red que existe a la sede B y sede C. **(Ver Anexo No AIR-011)**

Recomendamos que este mapa incluya en su diseño acotaciones o convenciones que faciliten la ilustración a cualquier persona que lo solicite, de igual forma se debe actualizar ya que hay contenido, diseño y componentes de la red que se omiten.

9. Organización de Documentación Administrativa

Dentro de la evaluación al manual de funciones y actividades, se observo que se carece de formalización y no se especifican los cargos de las personas que participan en la administración de la red y de la parte informática.

(Ver Anexo No AIR-012)

Se recomienda en lo mas pronto posible darle una formalización y obtener un documento que especifique las actividades de las personas encargadas de la red y generalmente del departamento de informática; para así tener en cuenta las funciones y actividades que cada uno debe desempeñar dentro de su área de trabajo.

10. Capacitación a los administradores de sala.

Los administradores que se encuentran en las distintas salas de computo de la Universidad, carecen de conocimientos básicos de la red, requiriéndose del apoyo del administrador principal para solucionar incidentes menores que los responsables de sala podrían solucionar. **(Ver Anexo No AIR-013)**

Recomendamos programar capacitaciones en soporte técnico de primer nivel liberando al administrador principal de estas labores básicas.

11. Mantenimiento a la red

Evidenciamos la falta de mantenimiento en cuanto a limpieza, etiquetado de cables, ajuste de canaletas, organización y eliminación de cables que no cumplen ninguna función. **(Ver Anexo No AIR-014)**

Se recomienda programar mantenimientos a la red semestralmente para evitar deterioro en los componentes físicos.

7.1.3 IDENTIFICACIÓN DE RIESGOS

Riesgo	ID	IMP	PRO	PONDE
Sabotaje y alteración de contraseñas en salas	R1	4	1	4
Acceso no autoriza a la red por cableado suelto	R2	5	2	10
Problemas de funcionamiento y organización por falta de identificación del cableado.	R3	3	4	12
Acceso no autorizado a switch	R4	4	2	8
Daños por suciedad o falta de mantenimiento al cuarto de telecomunicaciones de la sede G	R5	3	2	6
Incendios	R6	3	2	6
Sabotaje en los cuarto de telecomunicaciones.	R7	4	3	12
Libertad en las actividades de los funcionarios de informática.	R8	2	1	2
Corto circuito por falta de respaldo eléctrico Sede F	R9	4	4	12
Sabotaje a la red, Pinchazos e inseguridad.	R10	5	3	15

Tabla 7.2: Identificación de riesgos auditoria de red.

7.1.4 MATRICES DE RIESGO

PROBABILIDAD					
5					
4			R3	R9	
3				R7	R10
2			R5, R6	R4	R2
1		R8		R1	
	1	2	3	4	5

IMPACTO

Figura 6.1: Matriz de riesgos auditoria de red.

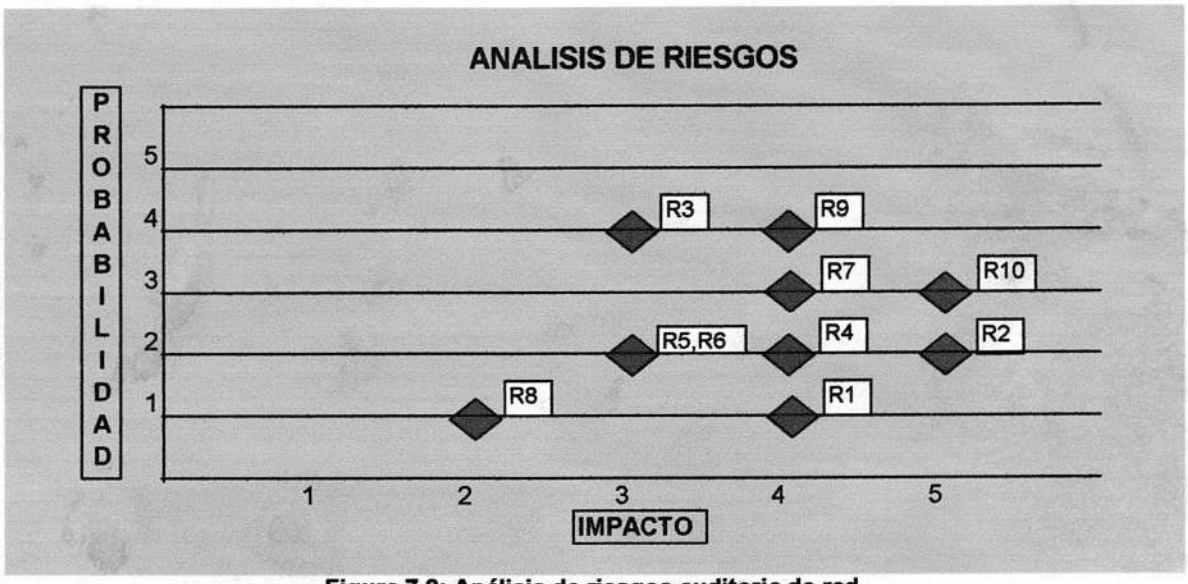

Figura 7.2: Análisis de riesgos auditoria de red.

7.1.5 CONCLUSIONES

Es muy importante el constante cambio que ha tenido la red de la Corporación Universitaria Unitec, pero carece de ciertos estándares fundamentales para el buen funcionamiento y estado de los componentes que hacen parte de esta, se hace salvedad que estos problemas se deben al surgimiento y crecimiento en tecnología para el beneficio de la universidad y la constante modificación de las terminales.

Sin embargo queremos destacar, la gestión, del departamento de informática y el administrador de la red, para la planeación, funcionamiento y seguridad, brindando, cada vez un mejor servicio a la comunidad Uniteista.

7.2 AUDITORIA APLICATIVOS EN DESARROLLO

7.2.1 INTRODUCCIÓN

Durante el período comprendido entre Abril 5 y Mayo 8 del 2005, se llevó a cabo un proceso de auditoria de aplicativos en desarrollo al modulo de admisiones y una breve revisión al ya implementado sistema de información general SIG de la CORPORACIÓN UNIVERSITARIA UNITEC, cuyos puntos principales fueron: análisis y cumplimiento de las etapas del ciclo de vida del sistema

Se utilizaron métodos de levantamiento de información como las entrevistas y la observación.

Así mismo, se presenta todo el procedimiento que se realizó y un informe final en el que se consignan los diferentes hallazgos, observaciones y obviamente las recomendaciones que el equipo auditor aporta para optimizar los diferentes recursos con que cuenta el sistema de información general.

7.2.2 INFORME FINAL AUDITORIA APLICATIVOS EN DESARROLLO

CORPORACION UNIVERSITARIA UNITEC
AUDITORIA INTEGRAL DE SISTEMAS
EVALUACIÓN DE APLICATIVOS EN DESARROLLO

I. OBJETIVO

Evaluar cada una de las etapas del ciclo de vida de sistemas de información para el aplicativo SIG (Sistema De Información General) de Unitec, determinando el cabal cumplimiento de las actividades en cada fase y su documentación.

II. ALCANCE

De acuerdo con la evaluación y verificación del modulo de Admisiones del aplicativo SIG (Sistema de Información General) se efectuaran recomendaciones para tener en cuenta dentro de la planeación, análisis, diseño y desarrollo del sistema.

La evaluación se realizó entre el 4 de Abril y el 8 de Mayo del 2005

III. OPORTUNIDADES DE MEJORAMIETO

De acuerdo con la información suministrada por el departamento de informática, realizamos un seguimiento minucioso al modulo de Admisiones del SIG que se esta implementado en la Universidad, obteniendo así un conocimiento general que permita brindar una serie de recomendaciones para su mejoramiento y optimización.

1. Cronograma de Actividades

Establecimos que el cronograma inicial de actividades fue realizado, sin detallarse concretamente el desarrollo de las actividades dentro del programa.

A la fecha de esta evaluación el cronograma se encuentra desactualizado.

Si este riesgo se llegara a materializar, esta situación, puede originar desorientación en el momento de comenzar a desarrollar el proyecto, incumplimiento en la entrega de avances estipulados en el proyecto y retrasos en la entrega del producto final.

En vista que el proyecto esta en curso, recomendamos aplicar un cronograma detallado y actualizado de las actividades, que facilite una mejor organización y control de las tareas a realizar dentro del desarrollo del programa.

2. Organización de Información

Evidenciamos que los documentos que hacen parte del levantamiento de información, para el desarrollo del SIG, se encuentran en una carpeta sin empastar, sin ganchos que le den un mayor agarre y seguridad.

En este caso se corre el riesgo de perder la información recolectada de manera fácil y en el momento de realizar una consulta no se lograría tener la información a tiempo.

Se recomienda, que esta documentación se encuentre en carpetas, folders, empastada o legajada, proporcionando mayor seguridad en los documentos físicos y existentes con los que cuenta el sistema de información.

Sugerimos también estructurar la organización de la información separándola por módulos.

Retroalimentación con Auditado

Se estableció con el Ingeniero Edgar Chamorro que la documentación del Sistema de Información general SIG se encuentra actualmente ordenada por módulos facilitando la consulta de los procesos y diagramas que lleva el sistema.

3. Copias de manuales de usuario

Se observó que los manuales de usuario, del SIG, están resguardados en los computadores de los programadores.

Ante un daño físico o lógico en los equipos donde se almacenan los manuales, existiría dificultad de recuperarlos. Para brindar soporte a usuarios, con la oportunidad y efectividad requerida.

Esta información debe estar almacenada en un dispositivo, a fin de disponer de una copia de respaldo externa, en el momento que se llegara a presentar un daño en los equipos o en la sala de informática.

Retroalimentación con Auditado

Evidenciamos y rectificamos junto con el Ingeniero Edgar Chamorro que existen backups de los manuales, software y bases de datos en CD'S, llevando una respectiva copia de seguridad.

IV. OPORTUNIDADES DE MEJORAMIENTO SEGUNDA FASE

Dentro de la auditoria que se realizo al modulo de admisiones, se llevo a cabo una evaluación detallada fase por fase al nuevo aplicativo.

FASE DE PLANEACION Y ANALISIS

1. Durante la evaluación y observación de la fase de análisis y planeación del modulo de admisiones se evidenció una herramienta de trabajo nueva para realizar la modelizacion de procesos del sistema actual y del sistema propuesto esta herramienta es UML.
2. Evidenciamos que el proyecto se encuentra debidamente estructurado en cuanto a la documentación redactado por los analistas y la suministrada por parte del departamento de informática.
3. Se Observó que existe conocimiento del área en el que se implementará el sistema y se tiene en cuenta la opinión y participación del usuario.

FASE DE DISEÑO

4. Se observo la implementación del plano de interfaz de usuario con estándares institucionales y un plano funcional del sistema suministrado por la Universidad.
5. Se observó la implementación de un modelo de representación gráfica del sistema llamado UML. Y un modelo constituido por análisis, diseño, codificación, pruebas y mantenimiento llamado Modelo secuencial lineal o también conocido como cascada.

FASE DE CONTRUCCION

6. Se evidenció y observó, en esta fase, el código fuente del programa con sus líneas y funciones comentariadas para tenerse en cuenta en el manual

técnico y en el futuro si este modulo llegase a tener cambios y modificaciones por otros analistas y programadores.

7. Se observó que esta ultima fase va de acuerdo con la fecha estipulada en el cronograma no existen retrasos por parte de los programadores y la documentación se encuentra al día.

7.2.3 IDENTIFICACIÓN DE RIESGOS

Riesgo	ID	IMP	PROB	PONDE
Falta del cronograma de actividades.	R1	4	1	4
Organización de información.	R2	4	2	8
Backup de manuales técnicos	R3	5	1	5

Tabla 7.3: Identificación de riesgos auditoria de aplicativos.

7.2.4 MATRICES DE RIESGO

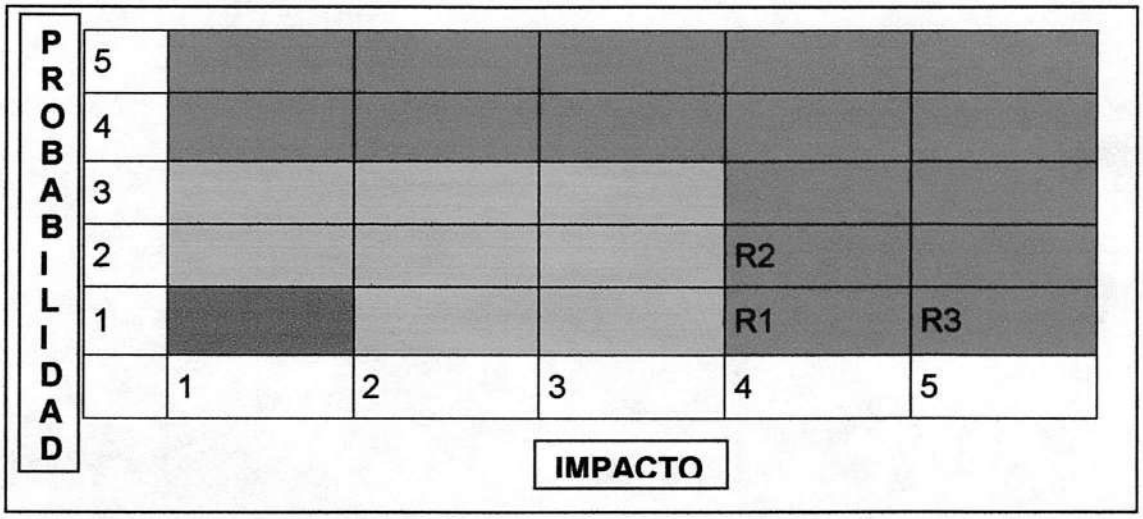

Figura 7.3: Matriz de riesgos auditoria de aplicativos.

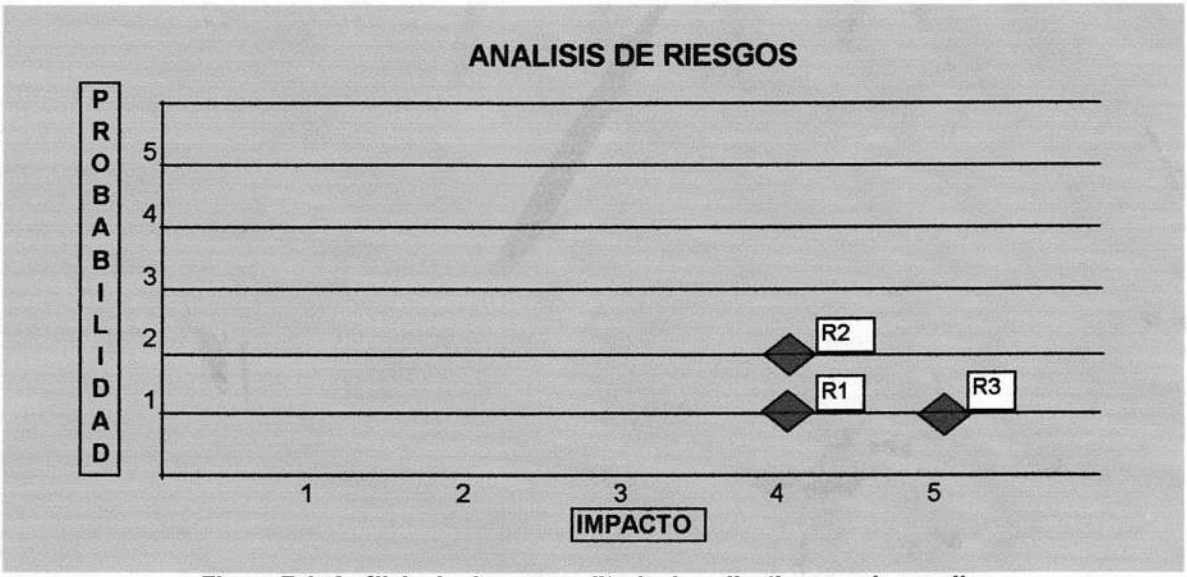

Figura 7.4: Análisis de riesgos auditoria de aplicativos en desarrollo.

7.2.5 CONCLUSIONES

De acuerdo a la evaluación y análisis de la auditoria de aplicativos en desarrollo que tuvo como objetivo realizar un seguimiento al Sistema de información general (SIG) y al modulo de admisiones, se observo que se lleva a cabo el cumplimiento y desarrollo de cada una de las fases del ciclo de vida del sistemas, destacando los procedimientos y estándares que se tuvieron en cuenta para el desarrollo del SIG y el modulo de admisiones.

Como valor agregado se evidencio el trabajo del departamento de informática para migrar y actualizar este sistema a web. Lo cual le daría a la universidad un cambio tecnológico importante para beneficio de los usuarios.

7.3 AUDITORIA FÍSICA

7.3.1 INTRODUCCIÓN

Durante el período comprendido entre Mayo 15 y Junio 12 de 2005, se llevó a cabo un proceso de auditoria física a la sede C de la CORPORACIÓN UNIVERSITARIA UNITEC, cuyos puntos principales fueron: accesos físicos, manejo de los equipos de cómputo, instalaciones del edificio y sistemas de seguridad.

Se utilizaron métodos de levantamiento de información como las entrevistas y la observación.

Así mismo, se presenta todo el procedimiento que se realizó y un informe final en el que se consignan los diferentes hallazgos, observaciones y obviamente las recomendaciones que el equipo auditor aporta para optimizar los diferentes recursos con que cuenta la sede C de la universidad.

7.3.2 INFORME FINAL AUDITORIA FÍSICA

CORPORACION UNIVERSITARIA UNITEC
AUDITORIA INTEGRAL DE SISTEMAS
EVALUACIÓN FÍSICA

I. OBJETIVO

Evaluar las condiciones físicas de la sede C de acuerdo a los estándares de seguridad que rigen sobre las instalaciones de los edificios en los que funcionan los centros de cómputo.

II. ALCANCE

La presente auditoria pretende evaluar las condiciones de la infraestructura de la sede C, en la cual se encuentran los laboratorios de informática de la Corporación Universitaria UNITEC, así mismo, los controles de acceso a ella y a los equipos.

De igual forma la ubicación del centro eléctrico, condiciones de seguridad tales como rutas de evacuación y planes de prevención y atención de incendios e inundaciones.

Este proceso inició el día 15 de Mayo y finalizó el día 12 de Junio del 2005.

III. OPORTUNIDADES DE MEJORAMIENTO

1. Cimientos de la Edificación

De acuerdo con el levantamiento de información, basado en la entrevista y la observación, se pudo establecer que la cimentación con la que cuenta el edificio, fue concebida para edificaciones de tipo familiar. Así mismo, el terreno sobre el

que se encuentra construido es un área que tiende a ceder, ya que este lugar presenta altos índices de humedad.

Si este riesgo se llega a materializar, es posible que la edificación sufra daños en la estructura y ceda.

Se recomienda realizar estudios anuales que permitan determinar el estado de la cimentación, proporcionando alternativas de mejora para su mantenimiento.

2. Sistema de Control Para el Préstamo de Equipos

Respecto del cuidado de los equipos y de las normas de seguridad que se deben tener en las salas que almacenan equipos, se pudo establecer la falta de control en el préstamo de equipos en horarios libres para los estudiantes.

Como consecuencia, encontramos que es muy probable que los equipos sufran daños físicos y lógicos.

Por lo tanto, se recomienda la implantación de un sistema por código de barras que capture datos del estudiante como, código, nombre, facultad y equipo de computo que le fue asignado.

3. Control de Ingreso

Con relación a este proceso, se pudo determinar que los sistemas de seguridad actuales no permiten una identificación confiable de los usuarios que ingresan al edificio, los estudiantes presentan la mitad del carnet mostrando solo el escudo de la universidad. **(Ver Anexo No AIF-001)**

En consecuencia se posibilita el acceso de personas ajenas a la facilitando la materialización de hurtos sobre archivos de la universidad.

Por esto sugerimos implantar nuevos sistemas de identificación o capacitar al personal de vigilancia para que aumente la exigencia en el acceso del personal.

4. Control de incendios

Existe un sistema de extintores distribuidos por la sede, sin embargo, no se tiene una identificación clara de su ubicación y se carece de rutas demarcadas de evacuación. **(Ver Anexo No AIF-002)**

En caso de ocurrir alguna eventualidad, se presentarían inconvenientes para la ubicación de extintores y evacuación de las personas que deben atender dichos eventos, dificultándoles el acceso a los equipos requeridos.

Se recomienda, demarcar las rutas de evacuación e implementar mapas de ayuda en la sede C.

5. Seguridad de los equipos de cómputo

Es notable, la falta de medidas de seguridad sobre los equipos de cómputo, ya que poseen un candado que es fácilmente vulnerable.

Existe el riesgo que los equipos puedan ser abierto por cualquier llave pequeña, lo que posibilita la sustracción de sus partes internas como discos duros, memorias, etc.

Se recomienda reforzar la seguridad de los candados que existen actualmente con otro tipo de sistema como guayas, cadenas, etc.

6. Capacitación Para la Prevención de Riesgos

Por medio de una entrevista establecimos la falta de capacitaciones a ciertos funcionarios que han ingresado en las ultimas fechas a laborar en la sede C.

Si llegase a existir cualquier tipo de emergencia estas personas no estarían en capacidad de brindar apoyo dentro de la sede .

Recomendamos se realicen jornadas preventivas a todos los funcionarios que trabajan en la Sede C incluyendo personal nuevo, con el fin de tener mas apoyo en el momento de una emergencia.

7. Simulacros de evacuación

Durante el tiempo que lleva en funcionamiento la Sede C, se observó la carencia de simulacros.

Existiría el riesgo que en el momento de una situación caótica, las personas que se encuentren realizando sus actividades en la sede no estarían preparadas para evacuar la edificación.

Se recomienda programar jornadas de simulacros para tener conocimiento de los procedimientos que deben tener en cuenta en un momento de emergencia.

8. Reubicación del Ingreso a la Sede C

Durante las visitas que se realizaron a la sede C, se observó que el ingreso de la comunidad uniteista y ajenos a ella se efectúa por la puerta occidental que esta junto a la entrada del departamento de informática. **(Ver Anexo No AIF-003)**

Esto podría aumentar la vulnerabilidad a la seguridad en el departamento ya que cualquier intruso accedería fácilmente a ocasionar robos, sabotajes etc.

Por lo tanto recomendamos que el ingreso de todas las personas sea por la puerta oriental que anteriormente se utilizaba y mantener distante el departamento de informática.

Retroalimentación con Auditado

Dentro de la reunión que se llevo a cabo con el jefe de seguridad, el doctor Luís Guillermo Vélez establecimos que el ingreso a la sede C no puede llevarse a cabo por la puerta oriental ya que en esta zona se encuentran activos valiosos para la universidad (Racks, equipos electrónicos, equipos de proyección, etc.).

Por lo tanto se ha evaluado y se ha considerado que el ingreso se realice por la puerta oriental.

9. Goteras en los Laboratorios de Informática

En el techo de la sede C existen Varios puntos donde se filtra el agua cuando llueve ocasionado así goteras dentro de los laboratorios de informática y el de electrónica de igual forma se observo que el techo es vulnerable ya que se puede levantar y no se encuentra parte de la teja. **(Ver Anexo No AIF-004)**

Existe el riesgo de que los equipos puedan sufrir daños por las goteras o de que cualquier intruso pueda acceder a la sede por el techo.

Recomendamos realizar un mantenimiento al techo revisando los puntos débiles y poder quitar estas goteras definitivamente.

7.3.3 IDENTIFICACIÓN DE RIESGOS

Riesgo	ID	IMP	PROB	PONDE
Desplome del edificio.	R1	5	2	10
Daños de los equipos partes físicas y lógicas.	R2	5	3	15
Acceso físico de intrusos.	R3	2	3	6
Incendio.	R4	4	3	12
Asalto/ Robo de equipos.	R5	3	5	15
Caos de Emergencia.	R6	2	4	8
Falta de Señalización.	R7	4	4	16
Ingreso de Intrusos al Departamento de Informática.	R8	4	2	8

Tabla 7.4: Identificación de riesgos auditoria física.

7.3.4 MATRICES DE RIESGO

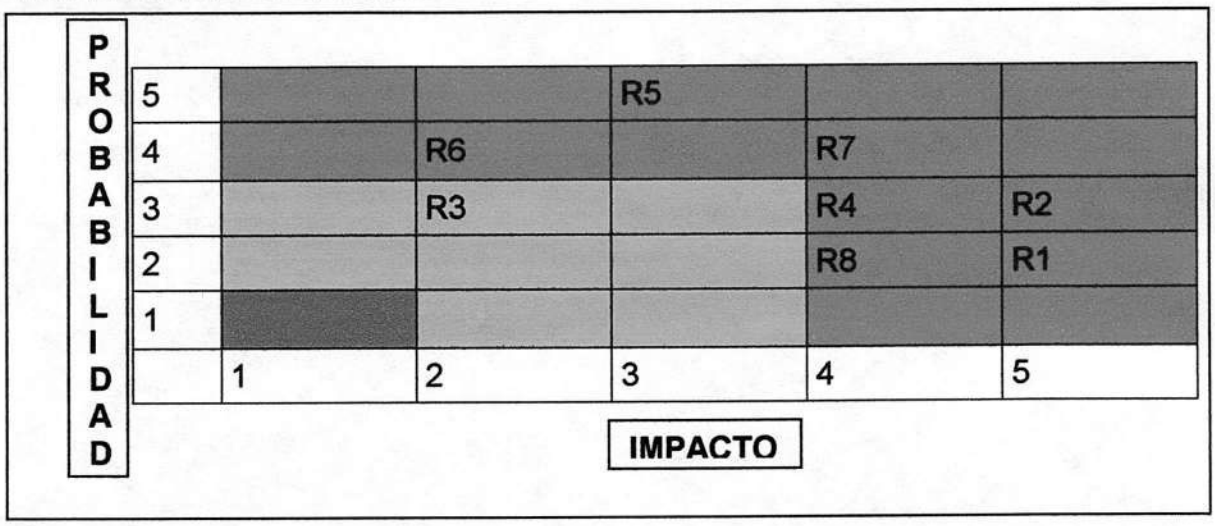

Figura 7.5: Matriz de riesgos auditoria física.

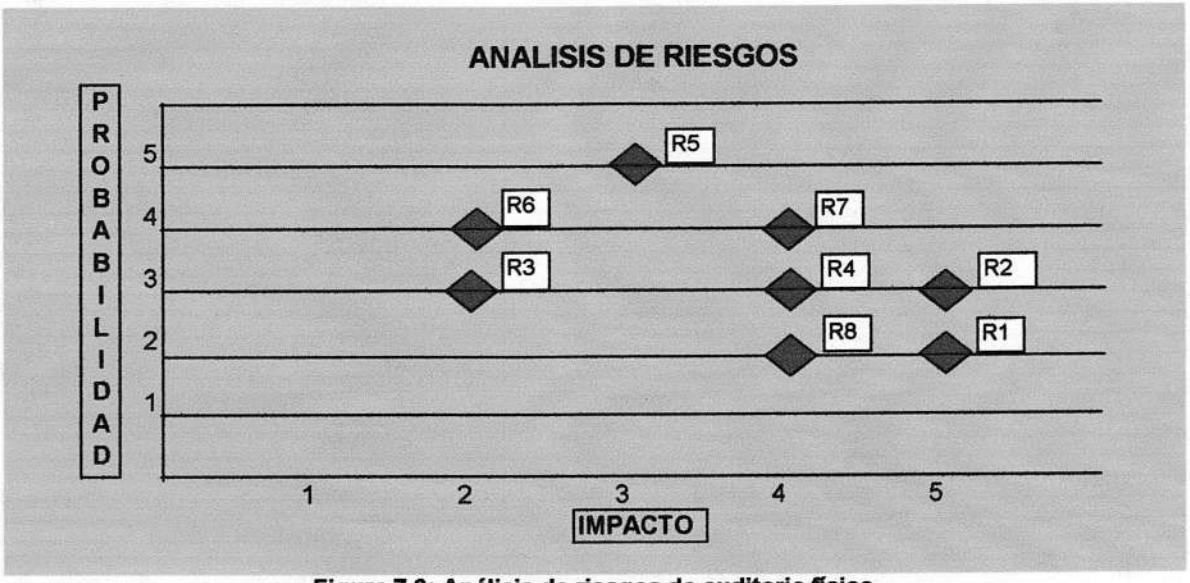

Figura 7.6: Análisis de riesgos de auditoria física.

7.3.5 CONCLUSIONES

Se han encontrado una serie de aspectos que demandan especial atención y requieren que sean implantadas las soluciones necesarias que puedan mitigar las debilidades que ella presenta; así mismo, se han elaborado una serie de recomendaciones que se encaminan a normalizar estos aspectos.

Sin embargo, es importante destacar como aspecto positivo no sólo los equipos y la capacidad de ellos, sino también, las medidas de seguridad tales como la implementación de alarmas a los equipos de elevado costo como los videobeams, equipos de electrónica, terminales y computadoras.

Capítulo 8
INFORME EJECUTIVO AUDITORIA INTEGRAL DE SISTEMAS

8.1 INTRODUCCIÓN

Durante el período comprendido entre Febrero 5 a Julio 10 del 2005, se llevó a cabo el proceso de auditoria integral de sistemas a la CORPORACIÓN UNIVERSITARIA UNITEC, cuyos puntos principales fueron: análisis y evaluación de la red, verificación del cumplimiento de las fases del ciclo de vida del sistema de información general SIG, y políticas de seguridad a la instalación física de la sede C.

Se utilizaron métodos de levantamiento de información como las entrevistas y la observación, fotografías y grabaciones.

Así mismo, se presenta todo el procedimiento que se realizó en un informe ejecutivo final en el que se consignan los diferentes hallazgos, observaciones y obviamente las recomendaciones que el equipo auditor aporta para optimizar los diferentes recursos con los que cuenta la universidad.

8.2 INFORME EJECUTIVO AUDITORIA INTEGRAL DE SISTEMAS

CORPORACION UNIVERSITARIA UNITEC
AUDITORIA INTEGRAL DE SISTEMAS
INFORME EJECUTIVO

I. OBJETIVO

Evaluar aspectos tecnológicos de la Corporación Universitaria Unitec, relacionados con el diseño, aprovechamiento, configuración y administración de la red, verificación de procedimientos adecuados para el desarrollo del sistema de información (SIG) y observación a la estructura física de la sede C comprobando su funcionalidad en cuanto a seguridad, protección e integridad.

II. ALCANCE

Evaluación de la distribución y configuración de la red, estándares implementados, componentes que la conforman y políticas de administración.

Comprobación de normas, procedimientos y documentación del ciclo de vida del sistema que garantice que el desarrollo del sistema de información SIG sea llevado a cabo.

Verificación de la confiabilidad física de la sede C evaluando control de accesos, identificación, instalaciones, recursos físicos y humanos teniendo en cuenta medidas de evacuación y alarmas para evitar riesgos considerados por la empresa o puesto de trabajo.

La auditoria integral de sistemas se efectuó desde el 5 de febrero hasta el 12 de junio del 2005.

III. OPORTUNIDADES DE MEJORAMIENTO

AUDITORIA DE RED

1. Identificación del Cableado

El cableado de las sedes B, E, G, F no se encuentra debidamente etiquetado ni Codificado. (Ver Anexo No AIR-002)

En este caso se corre el riesgo que los patch cord sean desconectados del switch o Patch panel y al conectar nuevamente se presenten problemas de funcionamiento y organización.

Se recomienda tener un etiquetado y a la vez una documentación del sistema de cableado instalado, en cada una de las sedes por lo cual se sugiere seguir la norma ANSI TIA/EIA 606. que garantiza una mejor administración de la red, y crear un método de seguimiento ya sea para traslados, cambios, adiciones facilitando la localización de fallas.

Se recomienda también verificar la identificación del cableado (C), closet de telecomunicaciones (TC), Áreas de trabajo (WA), en las sedes anteriormente nombradas.

Para cumplir esta norma se debe tener en cuenta la existencia de planos para ilustrar etapas diferentes de implementación e instalación ya sea conceptual o gráfica.

De igual forma se recomienda elaborar, en un software (Autocad), la ilustración grafica que especifique todos los ductos, elementos y rutas con una convención clara para el lector.

También se de debe tener en cuenta:

- Listar tanto al personal responsable de las operaciones físicas, como a aquellos responsables de actualizar la documentación.

Se recomienda etiquetar y listar todas las rutas y espacios a través de adhesivos o técnicas de inserción.

2. Reubicación de Switch

Evidenciamos que los Armarios, Racks y Switch carecen de una ubicación y climatización, en cada una de las Sedes de Unitec.

A continuación damos a conocer una tabla generalizada de la ubicación de las terminales en cada una de las sedes:

SEDE	PROBLEMA	RECOMENDACION
A	Observamos que los armarios que resguardan los switch, routers, módems carecen, de seguridad. (Ver Anexo No AIR-003) se evidencio que son de fácil acceso y junto a ellos se encuentran las llaves, y las puertas abiertas.	Recomendamos que las llaves sean guardadas en sitio remoto bajo la custodia del administrador.
B.	Evidenciamos que el Switch se encuentra situado en una esquina sobre el piso, acompañado de elementos como camisetas, trofeos, banderas, etc. (Ver Anexo No AIR-004) Este cuarto carece de condiciones adecuadas para el funcionamiento del Switch, corriéndose el riesgo que los cables sean desconectados o pisados, afectar la continuidad de las operaciones. Adicionalmente el cableado esta sin	Se recomienda que el Switch este por lo menos a un metro del piso, dentro de una caja metálica y el cableado este debidamente etiquetado y sin elementos alrededor de él.

	codificación ni etiquetado.	
E.	A través del estudio que se realizó en esta Sede, observamos que el Rack y el servidor se encuentran sobre el suelo, también se evidenció falta de organización del cableado en los Switch, no se cuenta con iluminación ni control de temperatura, el piso se encuentra alfombrado. (Ver Anexo No AIR-005)	Se recomienda la Reubicación de los componentes en un cuarto más amplio, mantener la parte eléctrica separada de la parte de datos e implementar controles de climatización, organización y etiquetado del cableado. Otra alternativa seria que los switch, Modems, etc. Se resguardaran dentro de un armario con seguridad y climatización para estos componentes.
F.	Apreciamos que el Rack se encuentra dentro de la misma sala del administrador, encima de una mesa auxiliar de escritorio, no existe organización ni etiquetado de cableado y el servidor DHCP se encuentra en el piso. (Ver Anexo No AIR-006) Existe el riesgo de que el Rack se caiga de la mesa o que sean desconectados los cables del Switch o Patch Panel ya que se encuentran a la mano de cualquier persona. De igual manera se observo que el piso de la sala es en caucho e inflamable y dentro de esta sede no se cuenta con una fuente eléctrica de respaldo para los equipos.	Es necesario disponer de un cuarto o armario apropiado para los componentes (Switch, servidor, módem, VPN etc) teniendo en cuenta condiciones ambientales, etiquetado y codificación de cableado.
G.	Observamos deficiencias en el estado de limpieza, organización y ambiente presentando problemas de humedad y suciedad que podrían afectar al Switch e interrumpir las actividades informáticas de la sede. (Ver Anexo No AIR-007)	Se recomienda remodelación, organización y limpieza a este cuarto y poner en funcionamiento el ventilador que se encuentra allí, para estabilizar la temperatura de este y así tener un lugar propicio para los componentes.

3. Adecuación de Closet de Telecomunicaciones

En las sedes A, B, E, G, F se carece de instalaciones adecuadas para los medios de telecomunicaciones (Switch, servidores, módems etc.) y los cuartos donde se encuentran situados estos componentes están desprovistos de control, seguridad y temperatura, entre otros. (Ver Anexo No AIR-008)

Establecimos inobservancia a la norma ANSI TIA/EIA-509 respecto a el edificio debe ser adaptable a cambios por configuración y/o expansión de la red, contar con Rutas de cableado Horizontal (Ductos bajo el piso, Piso Falso, Charolas para el Cable, Rutas de techo Falso), Rutas de cableado Vertical(en rutas intra e inter edificios), Closet de Telecomunicaciones, Cuarto de equipos, Entrada de Servidores, etc.

4. Mapa de Red

De acuerdo con el suministro de información por parte del departamento de informática, establecimos que hace falta orientar y delimitar los componentes tecnológicos que se encuentran en cada una de las Sedes de la Universidad; Dentro del mapa se deberá especificar la conexión de red que existe a la sede B y sede C. (Ver Anexo No AIR-011)

Recomendamos que este mapa incluya en su diseño acotaciones o convenciones que faciliten la ilustración a cualquier persona que lo solicite, de igual forma se debe actualizar ya que hay contenido, diseño y componentes de la red que se omiten.

AUDITORIA APLICATIVOS EN DESARROLLO

5. Organización de Información

Evidenciamos que la documentación que contiene el levantamiento de información, para el desarrollo del SIG, se encuentra en una carpeta sin empastar, sin ganchos que le den un mayor agarre y seguridad.

En este caso se corre el riesgo de perder la información recolectada de manera fácil y en el momento de realizar una consulta no se lograría tener la información a tiempo.

Se recomienda, que esta documentación se encuentre en carpetas, folders, empastada o legajada, proporcionando mayor seguridad en los documentos físicos y existentes con los que cuenta el sistema de información.

Sugerimos también estructurar la organización de la información separándola por módulos.

Retroalimentación con Auditado

Se estableció con el Ingeniero Edgar Chamorro que la documentación del Sistema de Información general SIG se encuentra actualmente ordenada por módulos facilitando la consulta de los procesos y diagramas que lleva el sistema.

6. Copias de manuales de usuario

Se observó que los manuales de usuario, del SIG, están resguardados en los computadores de los programadores.

Existe el riesgo que el computador perdiera la información por daños físicos (daños en el disco duro, corto circuito etc.) o lógicos (virus, bombas lógicas etc.).

Esta información debe estar almacenada en otro dispositivo de almacenamiento a fin de disponer de una copia de respaldo externa, en el momento que se llegara a presentar un daño en los equipos o en la sala de informática.

Retroalimentación con Auditado

Evidenciamos y rectificamos junto con el Ingeniero Edgar Chamorro que existen backups de los manuales, software y bases de datos en CD'S, llevando una respectiva copia de seguridad.

AUDITORIA FÍSICA

7. Sistema de control para el préstamo de equipos

Respecto del cuidado de los equipos y de las normas de seguridad que se deben tener en las salas que almacenan equipos, se pudo establecer la falta de control en el préstamo de equipos en horarios libres para los estudiantes.

Como consecuencia, encontramos que es muy probable que los equipos sufran daños físicos y lógicos.

por lo tanto se recomienda la implantación de un sistema por código de barras que capture datos del estudiante como, código, nombre, facultad y equipo de computo que le fue asignado.

8. Control de incendios

Existe un sistema de extintores distribuidos por la sede, sin embargo, no se tiene una identificación clara de su ubicación y se carece de rutas demarcadas de evacuación.

En caso de ocurrir alguna eventualidad, se presentarían inconvenientes para la ubicación de extintores y evacuación de las personas que deben atender dichos eventos se les dificultaría tener acceso a los equipos necesarios.

Se recomienda, demarcar las rutas de evacuación e implementar mapas de ayuda en la sede C. (Ver Anexo No AIF-002)

9. Simulacros de evacuación

Durante el tiempo que lleva en funcionamiento la Sede C, se observó la carencia de simulacros.

Existiría el riesgo que en el momento de una situación caótica, las personas que se encuentren realizando sus actividades en la sede no estarían preparadas para evacuar la edificación.

Se recomienda programar jornadas de simulacros para tener conocimiento de los procedimientos que deben tener en cuenta en un momento de emergencia.

10. Goteras en los Laboratorios de Informática

En el techo de la sede C existen Varios puntos donde se filtra el agua cuando llueve ocasionado así goteras dentro de los laboratorios de informática y el de electrónica de igual forma se observo que el techo es vulnerable ya que se puede levantar y no se encuentra parte de la teja. (Ver Anexo No AIF-004)

Existe el riesgo de que los equipos puedan sufrir daños por las goteras o de que cualquier intruso pueda acceder a la sede por el techo.

Recomendamos realizar un mantenimiento al techo revisando los puntos débiles y poder quitar estas goteras definitivamente.

11. Reubicación del ingreso a la sede C

Durante las visitas que se realizaron a la sede C, se observo que el ingreso de la comunidad uniteista y ajenos a ella, ingresan por la puerta que esta junto a la entrada del departamento de informática. (Ver Anexo No AIF-003)

Esto podría ocasionar falta de seguridad en el departamento ya que cualquier intruso accedería fácilmente a ocasionar robos, sabotajes etc.

Por lo tanto recomendamos que el ingreso de todas las personas sea por la puerta que anteriormente se utilizaba y mantener distante el departamento de informática.

8.3 IDENTIFICACION DE RIESGOS

Riesgo	ID	IMP	PROB	PONDE
Problemas de funcionamiento y organización por falta de identificación del cableado.	R1	3	4	12
Ubicación y adecuación de los armarios de telecomunicaciones.	R2	4	2	8
Adecuación de los cuartos de las terminales	R3	3	2	6
Diseño del mapa de red	R4	2	1	2
Organización de información.	R5	4	2	8
Backup de manuales técnicos	R6	5	1	5
Daños de los equipos partes físicas y lógicas.	R7	5	3	15
Acceso físico de intrusos.	R8	2	3	6
Ingreso de Intrusos al Departamento de Informática.	R9	4	2	8
Falta de Señalización en los extintores y salidas de emergencia.	R10	4	4	16
Desorientación en la evacuación en caso de emergencia	R11	4	2	8

Tabla 8.1: Identificación de riesgos auditoria integral de sistemas

8.4 MATRICES DE RIESGO

PROBABILIDAD						
	5					
	4			R1	R10	
	3		R8			R7
	2			R3	R2,R5,R9, R11	
	1		R4			R6
		1	2	3	4	5
			IMPACTO			

Figura 8.1: Matriz de riesgos auditoria integral de sistemas

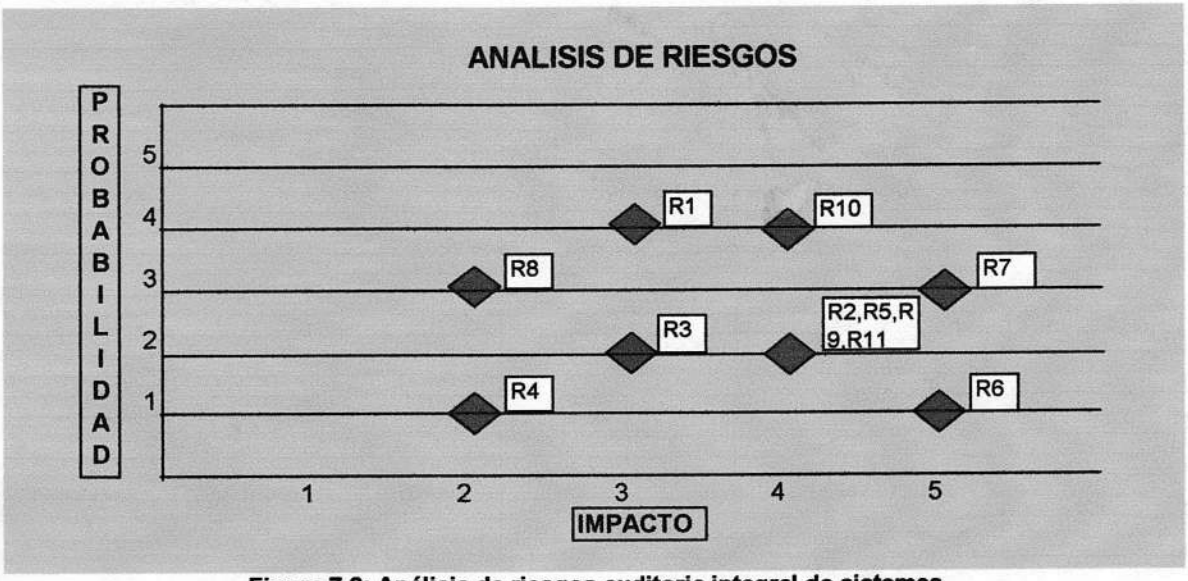

Figura 7.2: Análisis de riesgos auditoria integral de sistemas

8.5 CONCLUSIONES

Durante el proceso de evaluación de la auditoria integral de sistemas se analizaron tres aspectos importantes tecnológicos que actualmente se encuentran en surgimiento para el beneficio de las comunicaciones y aspectos informaticos de la Corporación Universitaria Unitec. Estos se evaluaron con el fin de emitir una recomendación que contribuya con el mejoramiento y crecimiento que se ha venido desarrollando a través de los años y con ayuda y colaboración del departamento de informática.

Capítulo 9
CONCLUSIONES

Durante el proceso de Auditoria Integral de Sistemas en la Corporación Universitaria Unitec, en el área de tecnología se evaluaron tres enfoques de auditoria informática:

- **Auditoria de Red** (Física, lógica y administrativa)
- **Auditoria de Aplicativos en Desarrollo** (Modulo de admisiones del SIG)
- **Auditoria Física** (Sede C)

Hallando así una serie de riegos que demandan una valoración y oportunidades de mejoramiento en cada una de las áreas auditadas, en las cuales se realizo un seguimiento evaluativo sistemático determinando la eficiencia y eficacia de los componentes, procesos y políticas comprendidos en cada enfoque.

Al termino de nuestra evaluación se ha realizado un informe ejecutivo integra los resultados obtenidos en las tres auditoria mencionadas anteriormente. Determinado así debilidades en cada una de las áreas auditadas.