****AUDITORIA DE SISTEMAS

AUDITORIA SALAS DE SISTEMAS DEL CITIS

AUDITORES

* Bote Vázquez Adolfo Natanael
* Macouzet Ortega Alfredo
* Pérez Gómez Vianney de los Ángeles
* Ramírez Azpeitia Isamar

Introducción

El Centro de Investigación en Tecnologías de Información y Sistemas (CITIS) es uno de los más grandes centros de investigación tecnológica en lo que a la universidad corresponde, en el presente trabajo se desglosaran las características en cuanto a infraestructura, tecnología y personal se refieran, a partí de esto se realizara una auditoria a la infraestructura, seguridad, planes de contingencia, manuales, enfocan doce en las aulas de computo en hardware y software, obteniendo así la información necesaria para plantear una propuesta que mejore el proceso administrativo de las tecnologías que se utilizan en este centro.

. Actualmente el CITIS se dedica a desarrollar proyectos de investigación en ciencias de la computación, en ciencias de la automatización y áreas afines, apoya la formación de especialistas en informática, automatización y control, desarrolla prototipos de aplicaciones informáticas y de automatización para solucionar problemas concretos, divulga los resultados de sus investigaciones y desarrollo tecnológico además de contar con aulas de cómputo en donde se imparten clases a estudiantes de diversas licenciaturas, esto gracias a que la tecnología que posee permite realizar correctamente cada una de las actividades antes planteadas.

Para hacer posible lo anterior, es indispensable elaborar una un diagnóstico apoyándose en las normas, formas y software de auditoria,

Índice

CAPITULO I INVESTIGACIÓN PRELIMINAR……………………………………………………………………………………….1

[1.1 A NIVEL DEL ÁREA DE INFORMÁTICA 2](#_Toc372056196)

[1.1.1 Visión 2](#_Toc372056197)

[1.1.2 Misión 2](#_Toc372056198)

[1.2 RECURSOS MATERIALES Y TÉCNICOS 3](#_Toc372056199)

[1.2.1 Estudios de viabilidad. 3](#_Toc372056200)

[1.2.2 Equipos 3](#_Toc372056201)

[1.2.3 Faces de instalación de los equipos y planes de instalación. 8](#_Toc372056202)

[1.2.4 Contratos vigentes de compra, renta y servicio de mantenimiento. 8](#_Toc372056203)

[1.2.5 Contratos de seguros. 8](#_Toc372056204)

[1.2.6 Convenios que se tienen con otras instalaciones. 9](#_Toc372056205)

[1.2.7 Configuración de los equipos y capacidades actuales y máximas. 9](#_Toc372056206)

[1.2.8 Planes de expansión. 9](#_Toc372056207)

[1.2.9 Ubicación general de los equipos. 9](#_Toc372056208)

[1.2.10 Políticas de operación. 9](#_Toc372056209)

[1.2.11 Políticas de uso de los equipos. 10](#_Toc372056210)

[1.3 SISTEMAS 10](#_Toc372056211)

[1.3.1 Manual de normas y procedimientos de los sistemas. 10](#_Toc372056212)

[1.3.2 Descripción genérica 10](#_Toc372056213)

[1.3.3 Diagramas de entrada, archivos, salida 10](#_Toc372056214)

[1.3.4 Salidas 10](#_Toc372056215)

[1.3.5 Fecha de instalación de los sistemas 10](#_Toc372056216)

[1.3.6 Proyecto de instalación de nuevos sistemas 11](#_Toc372056217)

[1.4 PERSONAL 11](#_Toc372056218)

[1.4.1 Perfiles del personal informático 12](#_Toc372056219)

[1.5 PLANEACIÓN DE LA AUDITORIA 13](#_Toc372056220)

[1.5.1 Pruebas de controles de los usuarios 13](#_Toc372056221)

[1.5.2 Pruebas Sustantivas 14](#_Toc372056222)

[1.5.3 Examen y evaluación de la información 15](#_Toc372056223)

[1.5.3.1 Evaluación de sistemas 15](#_Toc372056224)

[1.5.3.2 Evaluación del análisis 15](#_Toc372056225)

[1.5.3.3 Evaluación del diseño lógico 15](#_Toc372056226)

[1.5.3.4 Evaluación del desarrollo del sistema 16](#_Toc372056227)

[1.5.3.5 Control de proyectos 16](#_Toc372056228)

[1.5.3.6 Control de diseño de sistemas y programación 16](#_Toc372056229)

[1.5.3.7 Instructivos de Operación 16](#_Toc372056230)

[1.5.3.8 Forma de Implementación 16](#_Toc372056231)

[1.6 ENTREVISTA A USUARIOS 17](#_Toc372056232)

[1.7 CONTROLES 20](#_Toc372056233)

[1.7.1 Control de los datos fuente y manejo cifras de control 20](#_Toc372056234)

[1.7.2 Control de operación 21](#_Toc372056235)

[1.7.2.1 Controles de salida 21](#_Toc372056236)

[1.7.2.2 Control de medios de almacenamiento masivo 21](#_Toc372056237)

[1.7.3 Control de mantenimiento 22](#_Toc372056238)

[1.8 ORDEN EN EL CENTRO DE COMPUTÓ 22](#_Toc372056239)

[2.1.1 Institución: 25](#_Toc372056240)

[2.1.2 Servicios que brinda: 27](#_Toc372056241)

[2.1.3 ÁREA INFORMÁTICA. 28](#_Toc372056242)

[1.8 Organigrama 29](#_Toc372056243)

CAPITULO I

INVESTIGACIÓN

PRELIMINAR

# 1.1 A NIVEL DEL ÁREA DE INFORMÁTICA

## 1.1.1 Visión

Contribuir al desarrollo científico y tecnológico del Estado de Hidalgo, proponiendo soluciones inherentes a las ciencias computacionales, la automatización y control, tanto en el sector público como en el privado realizando investigación básica y aplicada en áreas estratégicas a las ciencias computacionales y del control y la automatización, maestría y doctorado.

## 1.1.2 Misión

En el Centro de Investigación en Tecnologías de Información y Sistemas (CITIS) se desarrollan diversos proyectos asociados con variadas líneas de investigación, además de que se imparten cursos de Especialización y Maestría en los diferentes programas de posgrado. El CITIS ofrece un plan de estudios de posgrado integral de alto nivel en ciencias de la computación y de la automatización y el control.

Las actividades más importantes de este Centro de Investigación son:

1. Elaboración y producción de materiales educativos.

2. Tutorías y asesorías al área académica y empresarial.

3. Desarrollo de proyectos de forma conjunta con los sectores productivo y social.

4. Vinculación externa con centros de investigación nacional e internacional.

# 1.2 RECURSOS MATERIALES Y TÉCNICOS

## 1.2.1 Estudios de viabilidad.

Para que se autorizara la construcción del CITIS primeramente se hizo un estudio de viabilidad que es el único que se ha elaborado en toda la historia del CITIS.

## 1.2.2 Equipos

El CITIS cuenta con equipo necesario para realizar las tareas de los docentes y alumnos.

* Aulas con equipo de proyección,
* Sala de usos múltiples, con capacidad para 50 personas.
* Salón siglo XXI, con 25 computadoras en red y equipadas con software de alta tecnología.

**Laboratorio software aula 4**

Cantidad

20 Computadoras

Monitor Fig. 3.1

Marca: Acer LCD Monitor

Modelo: No ALI916 C

Version: ALI916 cb

Characteristics: Rower Raiting ACI00-240V, 50-60 Hz, 10 A, 4 Puertos USB, Diskette, Lector CD

Mouse

Marca: Acer M-UVACR1

Modelo: MS MUV01005

Características: 5VDC 100mA

No. Serie: HC646030K52

CPU

Marca: Acer Veriton 5900 Pro

Teclado Acer

Modelo KV-0355

Cañón

Marca: SONY

Red

Mesas conectadas a un switch

No internet

Sin reguladores

Laboratorio De Computo Siglo XXI

Cantidad

26 Maquinas

Monitor

Marca: Dell CN-OY9833-71618-76P-AAYG

Modelo: REV A07

Características: Monitor 2 puertos USB

Teclado

Marca: Dell

Modelo SK-8115

Mouse Dell: M-UKDEL3

CPU: Optiplex 320

CD, DVD ROM

Diskette

Internet, Area Local

6 computadoras Acer no funcionan

20 Dell funcionando

3 Nobreaks

4 Lámparas, 9 Cuadros

24 Contactos de Red

Aula 2

Computadoras

Procesador: Intel inside Pentium 4

4 puertos USB

Teclado

Marca: Acer KV0355

Proyector de Acetato NOM-223 NYCE 3M

Laboratorio de Procesamiento de Imágenes

Cantidad

10 Maquinas

Monitor

Marca: Acer

Modelo: AL1916 C LCD Monitor

CPU

Procesador: Intel Pentium D Inside Vertion 5900 Pro

Características: 4 puertos USB, Lector CD, Diskette

Mouse

Marca: Acer MV-VACRI

Teclado

Marca: Acer KV-0355

No tiene Cañón

Sin red, internet

Laboratorio de Computo Inteligente

Cantidad:

20 computadoras

Monitor

Marca: HP

Modelo: 9500

CPU

Marca: HP

Modelo: HP Compaq

Características: Lector CD/DVD

1. Puertos USB MXJ5430278

Teclado

Marca: HP

Modelo: M-SK2880

Series: ASSY P/N 334084-002

Cañón

Tela del Cañón S/N Energía

Aula 7

* Sistema Operativo: Microsoft Windows XP Y Ubuntu
* Versión: 2002 service pack 3 (Windows)
* Ubuntu 10.10 maverick meerkat oct 2010
* Procesador:
* Intel Pentium4 CPU 3.00GHZ 2.99GHZ
* 504 MB de RAM
* Capacidad en disco duro: 23.9Gigabayte
* Número de Equipos: 20
* No cuenta con red
* Software:
* Adobe Flash player 11
* Adobe reader 7.0.8
* Avast Free antivirus
* Borldan c++ 5.0.2
* Microsoft Enterprise office
* Software Ubuntu
* Blender
* Brasero
* Open office

Aula 10

* Sistema operativo: Microsoft Windows XP
* Version: 2002 service pack 3 (Windows)
* Procesador:
* Intel Pentium D 3 CPU: 3.40GHZ
* 488MB RAM
* Capacidad en disco duro: 34.6Gigabaytes
* Número de equipos: 10
* No cuesta con red
* Software:
* Avast free antivirus
* Borland C++ 5.02
* Microsoft Enterprise office

## 1.2.3 Faces de instalación de los equipos y planes de instalación.

No aplica

## 1.2.4 Contratos vigentes de compra, renta y servicio de mantenimiento.

El único contrato vigente es el de la compara de 28 equipos de cómputo que fueron reemplazaron a otros 28 equipos que ya estaban deteriorados y recientemente fueron instalados en los laboratorios 7 y 10.

## 1.2.5 Contratos de seguros.

Actualmente el CITIS no cuenta con ningún tipo de seguro que proteja las instalaciones o el equipo.

## 1.2.6 Convenios que se tienen con otras instalaciones.

No existen convenios con otras instalaciones.

Solo se trabajan algunos proyectos que se gestionan ante CONACYT, y este proporciona los recursos necesarios.

## 1.2.7 Configuración de los equipos y capacidades actuales y máximas.

Se cuenta con un plan de configuración de los equipos que también especifica las capacidades actuales de las aulas, así como el número de equipos que se tienen actualmente.

## 1.2.8 Planes de expansión.

Actualmente se está trabajando en proyectos que están siendo desarrollados por Doctores investigadores y que posteriormente serán implementados en el centro de cómputo, como lo son proyectos financiados por Conacyt, para acrecentar los laboratorios, o crear nuevos laboratorios mejor equipados para un área de investigación especifica.

## 1.2.9 Ubicación general de los equipos.

Esta parte esta especificada en el plano de las instalaciones del CITIS.

## 1.2.10 Políticas de operación.

Dentro de la documentación del CITIS existe un apartado en el cual se describe el uso y que se le puede dar a las instalaciones, así como al área de cubículos y laboratorios.

## 1.2.11 Políticas de uso de los equipos.

El centro de cómputo cuenta con un reglamento que indica al usuario las condiciones de uso de los equipos y laboratorios, así como las limitantes de lo que puede cambiar en la configuración.

# 1.3 SISTEMAS

El centro de cómputo CITIS no cuenta con sistemas de operación, es decir no se cuenta con un sistema que permita validar a los usuarios, o que controle el acceso a los equipos, tampoco se tiene un sistema que permita a los usuarios reservar un equipo para hacer uso de el a determinada hora, por lo tanto no aplican los apartados de los siguientes puntos.

## 1.3.1 Manual de normas y procedimientos de los sistemas.

No Aplica

## 1.3.2 Descripción genérica

No Aplica

## 1.3.3 Diagramas de entrada, archivos, salida

No Aplica

## 1.3.4 Salidas

No Aplica

## 1.3.5 Fecha de instalación de los sistemas

No Aplica

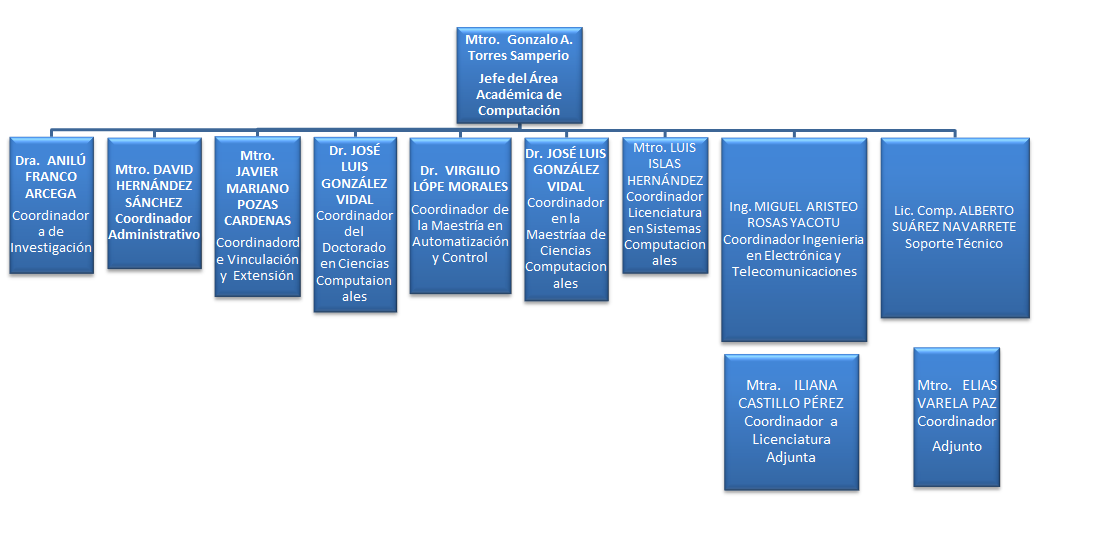
## 1.3.6 Proyecto de instalación de nuevos sistemas

No Aplica

En este caso se considera que el CITIS es un área que no necesita la implementación de un sistema de control, pues las labores que ahí se llevan a cabo no ameritan la implementación de este tipo de sistemas, los procesos desarrollados se pueden optimizar de otra manera e invertir ese tiempo y dinero para otros fines.

# 1.4 PERSONAL

En la figura se observa el organigrama organizado jerárquicamente, de manera horizontal el primer nivel está conformado por el jefe del área de computación, en el segundo nivel se encuentra el coordinador de investigación, administrativo, de vinculación y extensión, del doctorado en ciencias computacionales, de la maestría en automatización y control, de la maestría en ciencias computacionales, de la ingeniería en electrónica telecomunicaciones y el encargado de soporte técnico.

****

## 1.4.1 Perfiles del personal informático

El personal que conforma la plantilla de trabajo del CITIS está integrado por:

* 1 Ingeniero en telecomunicaciones.
* 5 Maestros en ciencias de la computación.
* 1 Doctora en computación.
* 1 Doctor en electrónica y control.
* 1 Maestro en administración.
* 1 Doctor en automatización.
* Doctores en ciencias.
* Maestros en ciencias.
* 1 Maestro en computación.
* 1 Maestro en electrónica.
* Licenciados en computación.
* Doctores en electrónica.

Los cuerpos académicos del Área Académica de computación son:

Computación Inteligente (en Formación), tres profesores

Data Mining

Sistemas Distribuidos y Paralelos

Electrónica y Control (consolidado), cuatro profesores

Sistemas Distribuidos

Sistemas No Lineales

Sistemas Lineales

Soft-Computing (en formación), tres profesores

Sistemas Inteligentes Distribuidos.

Sistemas Neurodifusos

Computación Educativa, (en proceso de registro), cinco profesores

Desarrollo de Software Educativo con Técnicas de Modelado de Realidad Virtual

Innovación y Evaluación Educativa

Microsistemas(en proceso de registro), tres profesores

Películas Sensoras y Dispositivos

Sistemas Microelectromecánicos Mems

# 1.5 PLANEACIÓN DE LA AUDITORIA

## 1.5.1 Pruebas de controles de los usuarios

**Analizar los controles establecidos y proponer otros controles**

En este punto se sabe que la persona que se encarga de diseñar y elaborar las pruebas para la información, es de la dirección de telecomunicaciones, (cuya sede se encuentra en CEVIDE) el departamento encargado de elaborar y aplicar estas pruebas, aquí cabe mencionar que son un conjunto de personas las cuales testean y administran las redes y telecomunicaciones de la UAEH. Es por esto que el encargado directo del CITIS desconoce esta información por que la señal llega de CEVIDE y estos aspectos corresponden al departamento de telecomunicaciones de la UAEH en CEVIDE, la red que llega a CITIS solo se le utiliza y da mantenimiento internó.

## 1.5.2 Pruebas Sustantivas

El CITIS se involucra muy poco o su participación es casi nula en este tipo de pruebas. La mayoría se llevan a cabo en CEVIDE una dependencia de la universidad que provee del servicio de redes.

1. Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.

Esta prueba si aplica ya que debido a que diversos incidentes el personal de telecomunicaciones, revisa que no se violen las reglas de confidencialidad en las redes y cabe destacar que son ellos los que están actuando en algunos casos en el papel del atacante en la red.

1. Pruebas para asegura la calidad de los datos.

Si aplica constantemente, pero son pocas y desconocen mucha información sobre los datos.

1. Pruebas para identificar la inconsistencia de los datos.

Esta no aplica

1. Pruebas para comparar con los datos o contadores físicos.

Si se realiza, pero no fue dada la información sobre cuáles son las que se realizan.

1. Confirmación de datos con fuentes externas.

Constantemente el personal de este departamento se encarga de fungir como atacante.

1. Pruebas para confirmar la adecuada comunicación.

También se realizan por el personal de este departamento. Y se aplican al azar en cualquier red de X instituto.

1. Pruebas para determinar la falta de seguridad.

Es una de las más interesantes en esta el mismo personal de este departamento se encarga de diseñar y elaborar estas pruebas también se toma en cuenta las experiencias de alumnos y los problemas que surgen a diario para testear este aspecto de seguridad de la red, y se simulan los ataques de manera sorpresa.

1. Pruebas para determinar problemas de legalidad.

Esta no aplica.

## 1.5.3 Examen y evaluación de la información

### 1.5.3.1 Evaluación de sistemas

En el CITIS no se cuenta con ningún sistema de información que ayude en las labores que se realizan, ni por el momento se tiene el proyecto de la implementación o desarrollo de algún sistema. Por lo tanto no se puede hacer una evaluación del análisis, del diseño lógico ni del desarrollo del sistema.

Tampoco se cuenta con ningún área de desarrollo de sistemas ni se tiene ningún proyecto de implementar esta área.

Más sin embargo según los usuarios si se necesitan, como en las entrevistas se menciona.

### 1.5.3.2 Evaluación del análisis

No aplica

### 1.5.3.3 Evaluación del diseño lógico

No aplica

### 1.5.3.4 Evaluación del desarrollo del sistema

No aplica

### 1.5.3.5 Control de proyectos

En el CITIS se desarrolla diversos proyectos realizados por los doctores que laboran en este lugar, y algunos de ellos incluyes a alumnos.

Para la asignación de recursos se tiene que hacer toda la documentación del proyecto y entregar al jefe de área académico quien en conjunto con el personal administrativo determina si se asignan recursos.

Algunos otros proyectos gestionan recursos a CONACYT, más sin embargo esto depende del proyecto.

E control de proyectos se lleva a cabo por el jefe de área académico y el contador, pero no existe un control muy claro y los periodos de entrega es acordado en el proyecto pero no se cumplen las fechas estipuladas.

### 1.5.3.6 Control de diseño de sistemas y programación

No aplica

### 1.5.3.7 Instructivos de Operación

No aplica

### 1.5.3.8 Forma de Implementación

No aplica

# 1.6 ENTREVISTA A USUARIOS

A continuación se presenta el cuestionario aplicado a los usuarios, no se aplicó a todos pero si a una muestra significativa. Las respuestas que se incluyen engloba lo que todos dicen, y en aquellas que preguntas que son cerradas se tomó lo que la mayoría describe.

1. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?.-   
Si (X ) No ( )   
¿Por que? Aunque no cumple del todo con aquello para lo que se supone fue creado, hay algunas deficiencias, si se utiliza para desempeñar la mayoría de las tareas que se requiere, no obstante se podrían aprovechar mejor las instalaciones.

2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?   
Deficiente ( )   
Aceptable (X )   
Satisfactorio ( )   
Excelente ( )   
¿Por que? En algunas ocasiones hay fallas en los aparatos y no hay nadie que pueda resolverlas o dar una referencia adecuada.

3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?   
No las cubre (X )   
Parcialmente ()   
La mayor parte ( )   
Todas ( )   
¿Por que? Porque no existe ningún sistema, pero debería de existir uno que facilitarían las cosas en departamento de presupuesto.

4. ¿Hay disponibilidad del departamento de cómputo para sus requerimientos?   
Generalmente no existe ( )   
Hay ocasionalmente ( )   
Regularmente (X )   
Siempre ( )   
¿Por que? Hay varias ocasiones donde ocurre una falla en mobiliario o equipo y no hay quien lo resuelva.

5. ¿Son entregados con puntualidad los trabajos?   
Nunca ( )   
Rara vez ( )   
Ocasionalmente ( )   
Generalmente (X )   
Siempre ( )   
¿Por que? Algunas veces se dan fechas para entregar alguna propuesta, pero salen del límite de entrega.

6. ¿Que piensa de la presentación de los trabajadores solicitados al departamento de cómputo?   
Deficiente (X )   
Aceptable (X )   
Satisfactorio ( )   
Excelente ( )   
¿Por que? Hay algunos perfiles que deberían llenarse para ciertas áreas o diversificar y no se cuenta estrictamente con ellos.

7. ¿Que piensa de la asesoría que se imparte sobre informática?   
No se proporciona ( X)   
Es insuficiente ( )   
Satisfactoria ( )   
Excelente ( )   
¿Por que? No se considera necesaria por las carreras que acuden al CITIS a tomar clases y sus usuarios en general poseen los conocimientos básicos.

8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que utiliza?   
Nula ( )   
Riesgosa ( X)   
Satisfactoria ( )   
Excelente ( )   
Lo desconoce ( )   
¿Por que? Creo que no hay ningún tipo de restricción en la red, no se manejan filtros ni similares, y la información en general es vulnerable.

9. ¿Existen fallas de exactitud en los procesos de información?   
¿Cuáles? No se sabe

10. ¿Cómo utiliza los reportes que se le proporcionan? No se han proporcionado reportes

11. ¿Cuáles no Utiliza?

12. De aquellos que no utiliza ¿por qué razón los recibe?

13. ¿Qué sugerencias presenta en cuanto a la eliminación de reportes modificación, fusión, división de reporte? Se debería modificar los reportes ya que para el fin de este centro no resultan de gran ayuda.

14. ¿Se cuenta con un manual de usuario por Sistema?   
SI ( ) NO ( X)

15. ¿Es claro y objetivo el manual del usuario?   
SI () NO ( ) No aplica

16. ¿Qué opinión tiene el manual? No ya manual de usuario.

17. ¿Quién interviene de su departamento en el diseño de sistemas? En general muchas son las aplicaciones que desarollan los doctores, pero propiamente no se tiene uno para el CITIS.

18. ¿Qué sistemas desearía que se incluyeran?

Algunos que ayude a llevar el control de proyectos y asignación de presupuesto.

Y otro para llevar un mejor control y poder hacer inventario del equipo de cómputo con que se cuenta

1. Observaciones:

En el CITIS se maneja gran cantidad de información, pero toda se mantiene en archivos, lo cual complica su administración

# 1.7 CONTROLES

## 1.7.1 Control de los datos fuente y manejo cifras de control

No aplica

## 1.7.2 Control de operación

### 1.7.2.1 Controles de salida

El CITIS cuenta con diversos controles de salida, en el caso de dispositivos electrónicos se elabora un pase de salida para dar mantenimiento preventivo o correctivo según sea el caso.

El encargado de retirar y reingresar dichos dispositivos el maestro Alberto Suarez Navarrete y el lugar de reparación de estos es en centro de cómputo académico.

La autorización de los pases de salida es emitida por el administrador de CITIS el contador David Sánchez Hernández y después de su autorización es necesario el registro en la bitácora de los encargados de seguridad física.

Al regreso del equipo los pases de salida son destruidos, verificando el buen funcionamiento de los dispositivos.

### 1.7.2.2 Control de medios de almacenamiento masivo

En CITIS se lleva a cabo un control de almacenamientos y resguardos de los bienes con los que cuenta, iniciando por su seguridad física la cual cuenta con aire acondicionado, sistemas de protección contra fuego (activos y pasivos), cerraduras especiales y privilegios de acceso a diferentes niveles.

El inventario de los dispositivos electrónicos y mobiliario, se realiza periódicamente y es monitoreado de igual manera.

Si llega a verse comprometido algún medio de almacenamiento se cuenta con un respaldo en el área de sistemas y un seguro para la sustitución del equipo.

En caso de que pase lo anterior se le da aviso al departamento jurídico, se deslindan responsabilidades y se levanta un acta.

## 1.7.3 Control de mantenimiento

En CITIS se realizan distintos mantenimientos preventivos y correctivos según sea el caso.

A continuación se muestra una tabla con el tipo de mantenimiento y su periodo en número de veces al año.

|  |  |  |
| --- | --- | --- |
| concepto | Tipo de mantenimiento | Periodo |
| Equipo de computo | Preventivo / correctivo | 2 |
| Aire acondicionado | Preventivo | 1 |
| Extintores | Preventivo | 1 |
| Mobiliario | Preventivo / correctivo | 2 |

En caso de mantenimientos correctivos el tiempo de respuesta para la verificación del desperfecto es de un máximo de 24 horas y el tiempo de reparación es ajeno a CITIS.

# 1.8 ORDEN EN EL CENTRO DE COMPUTÓ

El orden de CITIS está dado según las áreas de uso. Existen aulas de cómputo cercanas para su aprovechamiento, un apartado de cubículos para maestros y sus oficinas, un apartado para cubículos de alumnos y bodegas, un apartado para un laboratorio de electrónica o ciencias afines y por ultimo un apartado para las oficinas generales del inmueble.

El acceso a cada área está debidamente señalizado, para así poder restringir el uso de estas por personas ajenas a la institución, haciendo una excepción en congresos y talleres en los cuales se permite el acceso únicamente a aulas y el uso de equipo a terceros.

La limpieza del inmueble así como de los equipos en él, es llevada a cabo por el personal de limpieza universitario estando debidamente identificado.

CAPITULO II

AUDITORIA

INFORMÁTICA

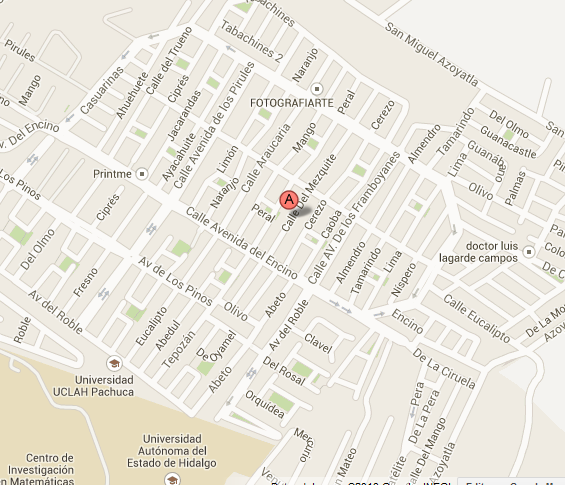
# 2.1.1 Institución:

**Logo:**

****

**Eslogan:**

*“Hacemos de la tecnologia tu mejor inversion.”*

****

**Direccion:**

**Calle Mezquite #326 Villas del Alamo, Mineral de la Reforma, Hidalgo C.P. 42184**

**Ubicación:**

**Reseña Historica:**

Auditec es una consultoria que nace en el 2009, cuando un grupo de jovenes emprendedores, decide crear una empresa de un giro diferente a las tipicas consultorias o desarrolladoras de software. Utilizando sus conocimientos técnicos para ayudar a las pequeñas , medianas y grandes empresas, a lograr sus objetivos y explotar los recursos tecnologicos con que cuentan.

A lo largo de este tiempo Auditec se ha dedicado a hacer estudios de la factibilidad que tiene la tecnologia en las empresas y desarrollar al maximo su potencial, tomando simpre como base los estandares internacinales.

En los ultimos años ha logra incursionar en el mundo tecnologico, como una buena opción debido a que ha resaltado por la calidad y profesionalismo con que se desempeña, permitiendo desarrollar proyectos para el sector publico y privado, en lugares como UAEH, el Hospital General de Pachuca Hidalgo, PGR, Intelsoft e inboxestudio.

**Web Site:**

www.auditec.com.mx

**Filosofia Institucional:**

El perseguir alcanzar el logro y avanzar en nuestros propósitos día con día constituye nuestra razón de ser como empresa.

Nuestros principios y valores con los cuales desempeñamos nuestro trabajo nos dan la personalidad, y forma de ser.

Como principio fundamental tenemos la perfección, origen y objetivo de las actividades que realizamos.

Es por todo eso que en auditec estamos comprometidos con el crecimiento del cliente mediante la auditoria informática de su empresa.

**Misión:**

Elaborar una evaluacion objetiva de las empresas, resaltando ante todo la etica, responsabilidad y preparacion con la cual nuestros auditores realizan su trabajo, detectando siempre las areas que podrian fortalecer la empresas, asi como sus carencias. Y de esta manera otorgar al cliente un panorama de los estandares con que labora su empresa.

**Visión:**

Convertirnos en la empresa de consultoria informatica número uno a nivel nacional, cumpliendo con los estandares internacionales de calidad y con el reconocimiento de los valores y etica con los cuales desempeñamos nuestro trabajo.

**Politicas de calidad:**

Todas nuestras auditorias se realizan basandose en estandares y normas internacionales reconocidas por la ISO (Organización Internacional de Normalización) y la IEC(Comisión Electrotécnica Internacional) entre otros.

# 2.1.2 Servicios que brinda:

* Auditoria en planes de contingencia
* Auditoria a los requerimientos mínimos de hardware
* Auditoria a los controles de seguridad y acceso al sistema
* Auditoria al soporte e instalaciones
* Auditoria a planes de mantenimiento preventivo y correctivo
* Auditoria en licenciamiento del software

# 2.1.3 ÁREA INFORMÁTICA.

El area informatica de CITIS se compone de 10 laboratorios, con las caracteristicas de hardware y software especificadas en el capitulo 1, el tipo de red con que cuenta es LAN, una antena de microondas de tipo parabolica y rack par procesar datos.

**AUDITORIA DE SISTEMAS**

**1.4. ORIGEN DE LA AUDITORIA**

La presente Auditoria se realiza en cumplimiento del Plan de Estudio que se tiene previsto para el periodo de Julio-Diciembre del 2013 en el CITIS aprobada mediante Plan de Estudios Auditoria al Procesamiento de Datos para la Licenciatura en Sistemas Computacionales. Asesor Lic. Comp. Adriana Katia López Hernández

**1.5. OBJETIVOS Y ALCANCE**

**1.5.1 OBJETIVO GENERAL**

Revisar y Evaluar los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

**1.5.2 OBJETIVOS ESPECIFICOS**

Verificación del sistema eléctrico de la sala de informática.

Verificación de la comunicación interna y externa (Lan, Wan o Man)

Verificación de Licencias y sus tipos.

Verificación Perfiles del cargo (personal competente).

Verificación de los elementos del hardware.

Verificación del control de las normas en la sala de informática.

Verificación de los Planes de contingencia.

Verificación de la diagramación de la red.

Verificación de la seguridad inalámbrica.

**1.6. ENFOQUE A UTILIZAR**

La presente acción de control, Pero este artículo goza de su propio desarrollo reglamentario materializado en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad., responsable de normar, supervisar y evaluar los métodos, procedimientos y técnicas estadísticas e informáticas, Normas Internacionales de Auditoria (NIA); habiéndose aplicado procedimientos de Auditoria que se consideraron necesarios de acuerdo a las circunstancias.

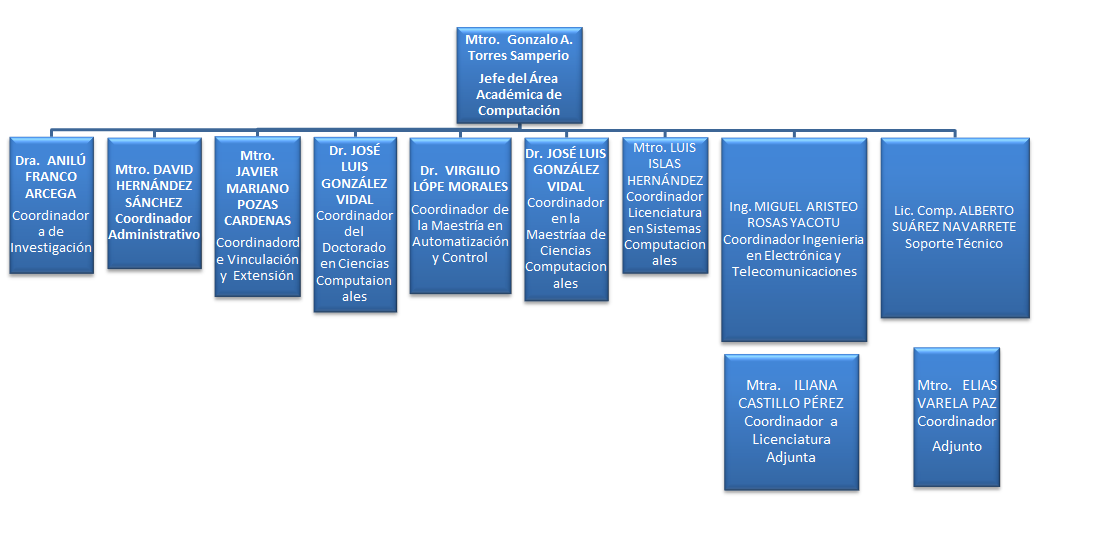
La presente Auditoria Informática se realizar en el CITIS siendo el área de Sistemas a examinarse.

**1.7. DOCUMENTOS A SOLICITAR**

* Políticas, estándares, normas y procedimientos.
* Plan de sistemas.
* Planes de seguridad y continuidad
* Contratos, pólizas de seguros.
* Organigrama y manual de funciones.
* Manuales de sistemas.
* Registros
* Entrevistas
* Archivos
* Requerimientos de Usuarios

## 1.8 Organigrama

En la figura se observa el organigrama que está conformado por niveles jerárquicos, de manera horizontal el primer nivel está conformado por el jefe del área de computación, en el segundo nivel se encuentra el coordinador de investigación, administrativo, de vinculación y extensión, del doctorado en ciencias computacionales, de la maestría en automatización y control, de la maestría en ciencias computacionales, de la ingeniería en electrónica telecomunicaciones y el encargado de soporte técnico.



**Fig. Organigrama**

**1.9. RELACION DE FUNCIONARIOS DEL AREA A EXAMINAR**

El personal que conforma la plantilla de trabajo del CITIS esta integrado por:

1 Ingeniero en telecomunicaciones.

5 Maestros en ciencias de la computación.

2 Licenciados en computación.

1 Doctora en computación.

1 Doctor en electrónica y control.

2 Doctores en electrónica.

1 Maestro en administración.

1 Doctor en automatización.

2 Doctores en ciencias.

1 Maestra en ciencias.

1 Maestro en ciencias.

1 Maestro en computación.

1 Maestro en electrónica.

Los cuerpos académicos del Área Académica de computación son:

Computación Inteligente (en Formación), tres profesores

Data Mining

Sistemas Distribuidos y Paralelos

Electrónica y Control (consolidado), cuatro profesores

Sistemas Distribuidos

Sistemas No Lineales

Sistemas Lineales

Soft-Computing (en formación), tres profesores

Sistemas Inteligentes Distribuidos.

Sistemas Neurodifusos

Computación Educativa, (en proceso de registro), cinco profesores

Desarrollo de Software Educativo con Técnicas de Modelado de Realidad Virtual

Innovación y Evaluación Educativa

Microsistemas(en proceso de registro), tres profesores

Películas Sensoras y Dispositivos

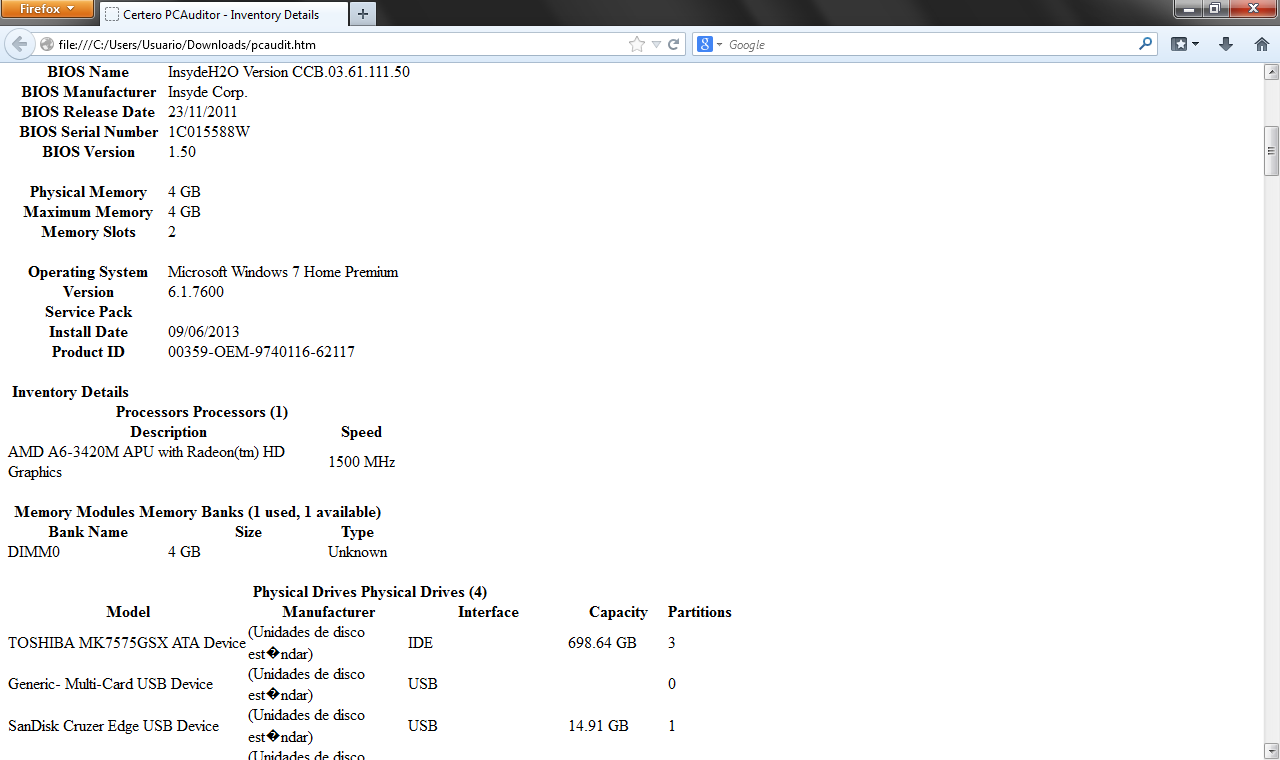
Sistemas Microelectromecánicos Mems

**1.10. TIPO DE SOFTWARE A UTILIZAR**

Se detallara el software utilizado para la verificación de licenciamiento del Software instalado en cada PC, cabe mencionar que solo se hizo el auditoria a maquinas al azar.

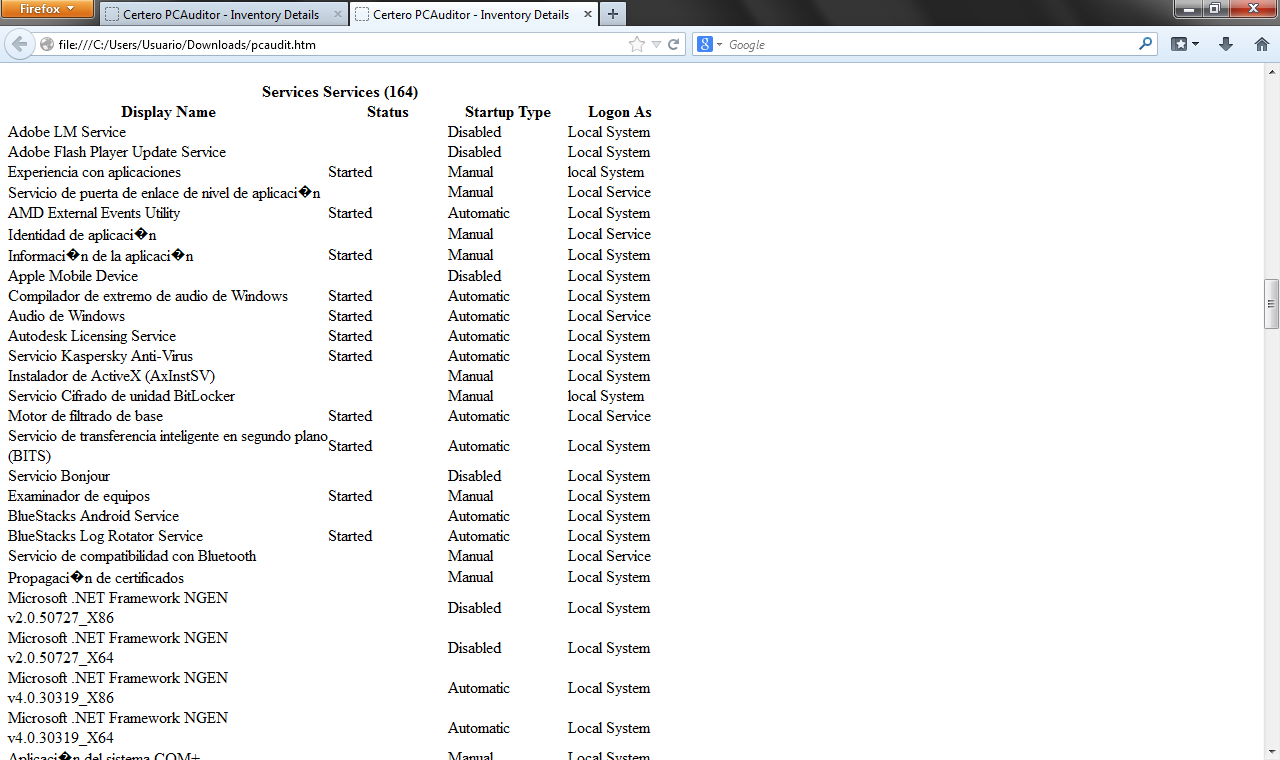
**1.7.1 CERTERO PCAUDITOR**

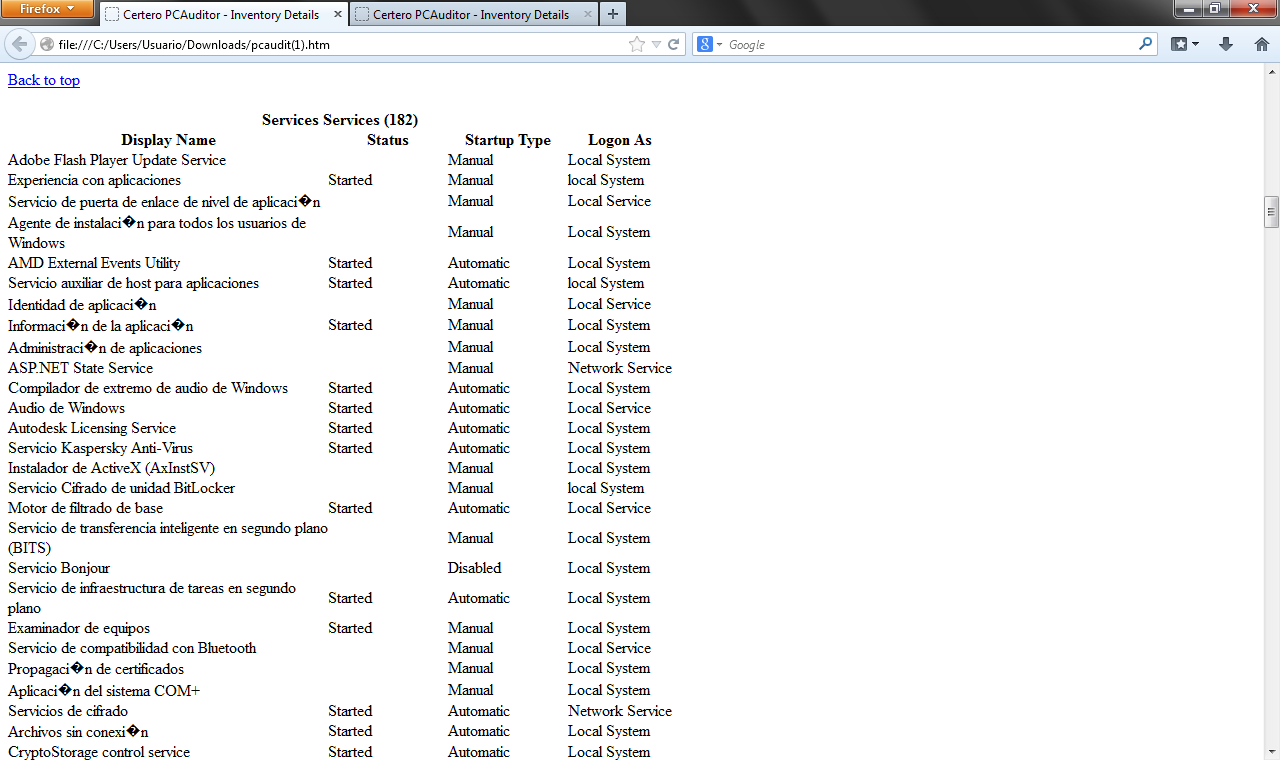
**HARDWARE**





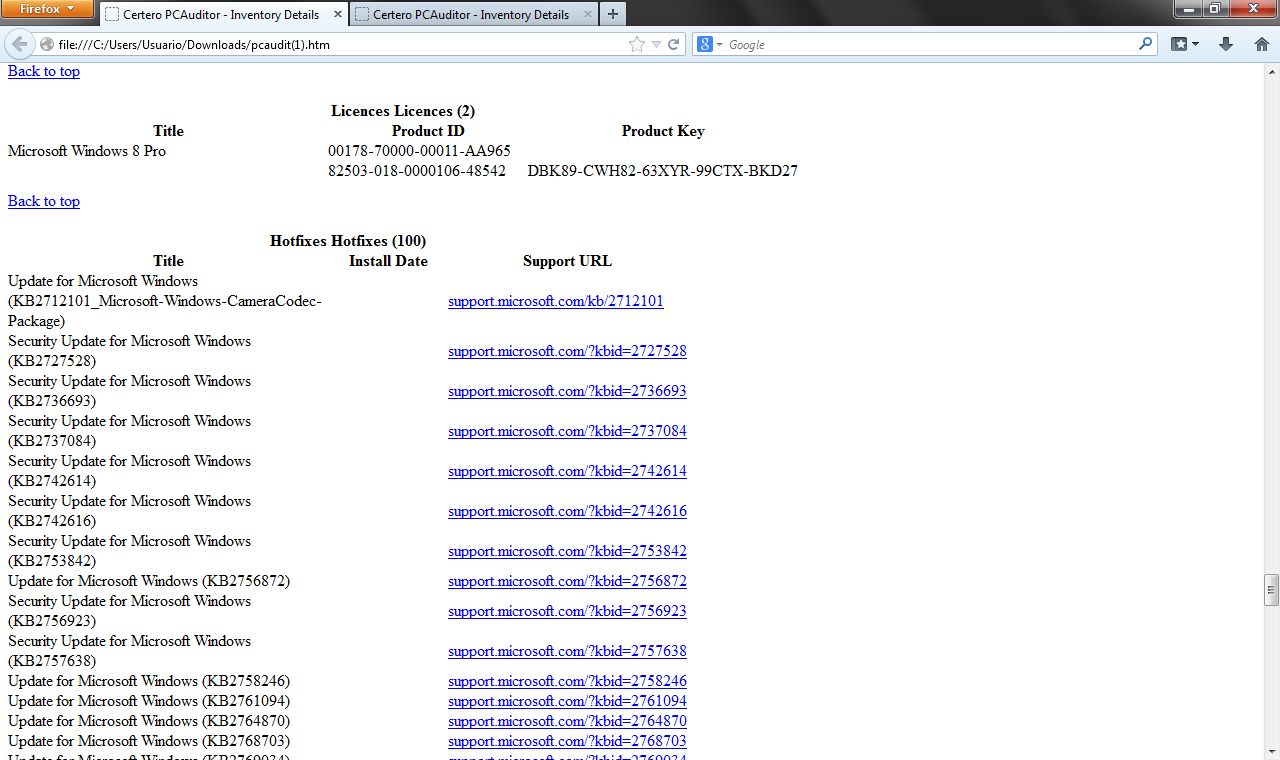
**SERVICES**





**LICENCIAS Y SOPORTES**





**2. INFORMES**

Dentro del informe estamos tomando los siguientes puntos como referencia, para ser auditados.

* Equipos de cómputo y su ubicación.
* Las conexiones eléctricas de los equipos de cómputo.
* Cableado estructurado.
* Conexiones de redes.
* Licenciamiento de Software informático.
* Planes de contingencia.
* Normas implementadas en las salas de informática.

2.1 Equipos de cómputo

Se cuentan con 7 salas de informática, las cuales serán auditadas de acuerdo a las normas que estén establecidas, se observará, y revisara de forma directa e indirecta los equipos, su instalación, ubicación y funcionamiento de las mismas.

Las cuales están bajo la responsabilidad del Mtro. David Hernández Sánchez.

2.1.1 Cuantos equipos existen.

|  |  |
| --- | --- |
| Numero de monitores | Numero de torres (CPU) |
| 126 | 126 |

Características de conexión de los equipos en cuanto al cableado de cada uno.

Todos los equipos cuentan con una conexión eléctrica en la mesa en la que se ubica, la cual está aterrizada a una tierra física para evitar que las descargas eléctricas o variaciones en el voltaje, dañen los equipos de cómputo, además se cuenta con un cableado de red de tipo bus, el cuan se encuentra conectado a un rack que se ubica bajo resguardo en el segundo piso.

* Monitor (cable de energía /cable VGA).
* Torre (cable de energía).
* Mouse (USB),
* Teclado (USB).
* UPS (no disponible en todos los equipos).
* Reguladores de Voltaje (no disponible en todos los equipos).

3 Puntos débiles y amenazas

FODA

|  |  |  |
| --- | --- | --- |
|  | Fortalezas | Debilidades |
| Análisis Interno | Aulas de computo separadas  Aulas equipadas  Equipo propio  Equipos completos  Encargado de soporte  Licencias de software | Equipo obsoleto  Equipo descuidado  Usuarios irresponsables  Falta de actualización en el sistema operativo  Versiones obsoletas de software  Equipos de cómputo lentos  No todos los equipos cuentan con reguladores y/o no-break |
|  | Oportunidades | Amenazas |
| Análisis externo | Adquisición de nuevas tecnologías  Campañas de orientación sobre el uso de los equipos  Utilización de software de licencia libre. | Desarrollo de nuevas tecnologías en el mercado  Desaprobación de planes económicos |

3.1 Recomendaciones de la auditoria

Desarrollar campañas de orientación de uso de equipos, tanto para los alumnos, como para los catedráticos y personal externo a la organización.

Agilizar los equipos de cómputo mediante las actualizaciones correspondientes, tanto de sistema como de software de licencia.

Adquisición de equipos para la seguridad en la corriente eléctrica.

4 Conexiones eléctricas.

Después de recorrer las salas de cómputo, hemos podido detallar que no existe una correcta instalación eléctrica para los diferentes equipos y dispositivos que se manejan en las salas de sistemas.

Para el correcto funcionamiento del sistema de corriente eléctrica se recomienda consultar la Norma Técnica Colombiana NTC 2050 en la sección 645 que se refiere a las instalaciones eléctricas en equipos informáticos.

4.1 puntos débiles y amenazas

* No existen equipos personales para la protección de descargas eléctricas (reguladores de voltaje).
* Contactos no disponibles para equipos externos que requieran una conexión eléctrica.
* El cableado se ubica sobre las mesas, lo que impide que se puedan realizar maniobras, ya que se tendría que desmontar todo el sistema de corriente eléctrica.

4.2 Recomendaciones

Con base en la NTC 2050 se recomienda:

* La utilización de pisos falsos para colocar las conexiones eléctricas por debajo de las mesas (645-5).
* Proteger las conexiones contra daños físicos (645-5).

5 Cableado estructurado

La conexión de redes con la que cuenta este centro de investigaciones, es diferente dependiendo los laboratorios. A continuación se describirá el tipo de conexión que tiene cada una de las aulas.

Laboratorio aula 4

En este laboratorio se cuenta con 20 Maquinas, todas las maquinas se encuentran conectadas en red, las cuales se concentran en un switch de 48 puertos. Cabe mencionar que estas máquinas solo están conectas a una red de área local, ya que no cuentan con conexión a internet.

Laboratorio De Computo Siglo XXI

Este laboratorio tiene 26 Maquinas, de las cuales solo 24 se encuentran conectadas en red. Están conectadas mediante un switch, a una red LAN, estos equipos si cuentan con una conexión estable a internet.

Aula 2

Esta aula, no cuenta con ningún tipo de conexión en red aunque el cableado físico si se encuentra.

Laboratorio de Procesamiento de Imágenes

Este laboratorio cuanta con 10 Maquinas, que solo cuentan con cableado físico ya que no se encuentran conectadas de ninguna forma, ni a una red LAN ni con acceso a internet.

Laboratorio de Computo Inteligente

El laboratorio de computo inteligente cuenta con 20 Maquinas, el cual cuenta con el cableado físico en cada una de las maquinas, cuenta con una conexión LAN y la mayoría de los equipos si cuentan con una conexión a internet, aunque de manera inestable.

5.1 Puntos débiles y amenazas

* Las conexiones a internet y entre computadoras son muy lentas.
* El cableado en algunas salas esta visible al usuario.

5.2 Recomendaciones

* Mejorar el servicio de internet, de esta manera las actualizaciones pueden hacerse de manera automática, lo que mejoraría la calidad de vida de los equipos.
* Proteger el cableado contra daño físico.

6 conexiones de redes

En algunas áreas se encuentran Switch para la conexión de redes además se cuenta con un rack que está destinado a alojar el equipamiento eléctrico útil para procesar datos, ya que se necesita alojar un gran número de dispositivos.

Modulo: LAN scape.

Campania: Corning Cable Systems.

No. De Serie CITIS: NS CATO926KL6R



6.1 Amenazas y debilidades

* No se cuenta con un SITE en el cual se resguarde el rack, por lo que cualquiera que entre a la sala de juntas podría manipular y alterar el funcionamiento de dicho equipo.

6.2 Recomendaciones

* Se recomienda la creación de un SITE para resguardo del rack, de esta manera solo personal autorizado de mantenimiento puede manipular el equipo.

**7.2. PLANES DE CONTINGENCIA.**

Actualmente no existe un plan de contingencia en el centro de cómputo ni ningún otro plan que considere los posibles riesgos.

***Planes de contingencia (propuesta)***

* El primer punto a tratar es referente al software el principal riesgo que existe en este ámbito es la perdida de información que podría darse ya que en algunos casos los virus que se han alojado en algunas máquinas son suficientes para que un equipo tarde en responder o peor aún el riesgo mayor es el de perder información.

Para poder responder de manera adecuada a esto tipo de riesgos la base de datos del CITIS será respaldada diariamente en forma automática y manual, según los procedimientos generados para tal efecto.

* El otro punto a considerar es a nivel Hardware ya que podría suceder un brusco cambio en el voltaje que pudiese inutilizar ciertas maquinas, para esto se debe contar con el respaldo, pero también se cuenta con un plan de financiamiento para que en caso de que esto llegara a suceder se pudiesen reemplazar estas máquinas.

Las fuentes de financiamiento pueden ser principalmente de instituciones bancarias a través de créditos. Para el caso de centros de cómputo destinados a la educación públicas no existen fuentes de financiamiento, a menos que la institución educativa cuente con un área destinada a la producción de software para empresas privadas, entonces la misma empresa puede ser el origen del financiamiento.

En caso del CITIS este obtiene su financiamiento a través de los recursos que son enviados por el gobierno federal y Estatal así como del conocí para el desarrollo de proyectos y una pequeña parte de las empresas asociadas a la universidad como son:

• Patronato UAEH.

• La imprenta universitaria.

• Radio universidad.

**7.2.1. PUNTOS DÉBILES Y AMENAZAS.**

Hay varias debilidades detectadas en el centro de cómputo no obstante la más grave es la falta de respaldo de información de vital importancia para la organización como lo son los planes administrativos, los gastos del CITIS las propuestas de los investigadores y toda la información que genera la organización, también está el auditar y llevar un control de la forma en la que se utilizan los equipos de cómputo mediante la activación de una herramienta que viene en Windows ya que con esto se lograría detectar aquellos comportamientos que representen un amenaza para la organización.

Otra aspecto que representa un grave riesgo para la información es la falta de mantenimiento ya que debido al acceso que tienen los alumnos y un gran número de personas externas a la universidad que ingresan al centro de cómputo favorece el ambiente para el contagio de virus que ponen en riesgo no solo la información sino también la configuración de estos equipos el mantenimiento es importante al igual que la depuración de las carpetas de archivos cada semana para evitar que se quede en las maquinas información que ya no se utilizara y que solo hace lentas a las maquinas.

Otra amenaza de la que ya se tienen antecedentes son las posibles fallas de voltaje ocurridas en el equipo de cómputo en el pasado que podrían quemar las computadoras, para esto se debe contar con un plan de financiamiento y de esta forma poder reemplazar las maquinas obsoletas.

**7.2.2. RECOMENDACIONES**

Lo más importante y que se debe resaltar es la importancia que tiene la ejecución de los planes de mantenimiento para el centro de cómputo ya que es precisamente esto lo que ha llevado a que los equipos de cómputo prácticamente no se utilicen debido a la falta de velocidad de las máquinas para responder y procesar información así como los virus que se propagan de manera muy rápida por la red y puertos de las maquinas. Si este mantenimiento no se lleva a cabo prácticamente no tiene caso el resto del trabajo.

**7.3. NORMAS PARA USO DE LAS SALAS DE SISTEMAS**

Al interactuar con los alumnos que ingresan al centro de cómputo se puede observar que hay muchos académicos que no se registran este es el principal así como la falta de mantenimiento y tanto de software como de hardware.

Tampoco se cuanta con reportes para mencionar las posibles fallas de los equipos.

Este también es un aspecto práctico que debería de considerase dentro del mantenimiento

*GENERAR UN REGLAMENTO DEL USO DE LOS EQUIPOS DE CÓMPUTO*

*1.- al ingresar al centro de cómputo portar siempre su credencial en una parte visible.*

*2.- registrarse siempre como usuarios dentro de un sistema de bitácoras, registrar el nombre y datos de gran importancia.*

*3.- se debe guardar todo documento en la ruta adecuada.*

*4.- deberá guardarse el historial de documento y cambiarse cada cierto tiempo.*

*5.- Dar buen uso al equipo de cómputo.*

*(Encendido y apagado).*

*6.- La información generada deberá ser depurada cada mes.*

*7.- Ingresar siempre en la cuenta de usuario y no de administración ya que será esta la que contara con los programas instalados que se requieren para los programas de los semestres que utilizaran dicho laboratorio.*

PROPUESTA

**Capítulo 1 definiciones**

**Equipo computacional académico**Se considera como equipo computacional de uso académico a todo aquel equipo de cómputo, accesorio, periférico, de telecomunicaciones o relacionado con cualquiera de éstos, que esté instalado en las salas o laboratorios de acceso común y que estén destinados al uso por parte de los usuarios académicos.

**Equipo computacional administrativo**Es todo aquel equipo adquirido por la universidad en el área académica de computación y destinado a servir como apoyo a labores administrativas del personal del CITIS. Dentro de esta categoría se considera el equipo instalado en las oficinas Administración cuyo jefe es el Mtro. David Hernández Sánchez.

**Usuarios académicos**Se consideran usuarios académicos de los servicios de cómputo de la Dirección de Informática a:

* Los alumnos de la Licenciatura en sistemas computacionales y La ingeniería en electrónica y telecomunicaciones.
* Todos los alumnos de las maestrías impartidas en esta área Maestría en Ciencias computacionales, Maestría en Automatización y control y el resto de los programas académicos a cubrir por estas áreas del cuerpo académico de computación.

**Usuarios administrativos**Se consideran usuarios administrativos a:

* Los empleados, profesionistas de apoyo y directivos que hagan uso de los servicios del Centro de Computo Académico como apoyo a sus actividades laborales.

**Uso académico**Se considera uso académico del equipo computacional y de comunicaciones a aquél que sirva como apoyo a la elaboración, solución, investigación de tareas, proyectos o trabajos relacionados directamente con cursos regulares impartidos en el área académica de computación, así como el destinado a la preparación de material de apoyo a los mismos, y comunicación electrónica con otros usuarios académicos.

**Capítulo 2** ***uso de los equipos de cómputo académicos***

El equipo computacional académico deberá utilizarse únicamente como herramienta de apoyo para la realización de labores académicas de los alumnos.

Cualquier otra persona que no sea considerada como alumno deberá solicitar un permiso en la dirección de administración para poder utilizar los equipos de cómputo de esta área.

En el caso de que sea un alumno el que desee utilizar los equipos de cómputo en un futuro bastara con presentar su credencial o tira de materias vigente.

**Capítulo 3** Acceso a las áreas de servicio de cómputo académico

En esta área únicamente se permite el acceso a alumnos que puedan realizar tareas académicas o investigaciones haciendo buen uso del equipo.

Un alumno deberá registrarse en el sistema de control para poder avisar por cuanto tiempo utilizara el equipo.

Para que el alumno pueda tener total acceso a estas áreas también deberá portar su credencial en un lugar vistoso credencial del periodo vigente actual donde cada uno de sus rasgos deberán apreciarse en su totalidad, la fotografía deber ser reciente y además se contara con un sistema de pre registro al momento de ingresar al aula para anotar a cada alumno y su posición.

**Capítulo 4** Acceso a los servicios en equipos de cómputo centrales y servicios de red

El principal uso que se hace a este laboratorio es el uso de las máquinas para consultas vía internet y acceso a los servicios en equipos de cómputo centrales y servicios de red, esto claro está en función ya se tiene establecido ya en el departamento de redes y Telecomunicaciones de la UAEH.

En este punto se considerara el uso de la red que es lo principal en esta área.

En el campus se considera el préstamo de equipos de cómputo a personas ajenas a estas áreas, para poder reservar una computadora bastara con poner el número de posición en la cual podemos solicitar un lugar basto con registrarse al ingresar.

**Capítulo 5** Comportamiento a observar

Los usuarios alumnos que ingresan a los centros de cómputo deberán de dar un buen uso a las máquinas para esto es que se activara la herramienta que se mencionó con anterioridad en otros capítulos, de esta forma se detectara si existen usuarios que están dando un mal uso o si tienen un comportamiento sospechoso y de esta forma se procederá a activar las medidas de seguridad como actualización de antivirus y desinfección de máquinas que cuando tiene algún virus únicamente se dejan de lado y prácticamente se vuelven inutilizables.

También se deberá monitorear que en efecto hayan sido utilizadas para fines escolares durante el horario de uso ya que hay algunos alumnos que únicamente utilizan a las máquinas para jugar durante el horario que se supone debiera ser de clases.

**Capítulo 6** separación de equipos o equipos con acceso restringido

La división de equipos de cómputo se realizara únicamente para llevar un control en las aulas que diferencie a maestros de alumnos, por ejemplo si se debe realizar algún trabajo o practica que requiera de un instructor se podría realizar dicha separación.

Y esta solicitud deberá ser presentada por escrito por el docente al jefe de administración así como al encargado de mantenimiento para que instale la paquetería necesaria y verifique la red y de esta manera se tenga todo preparado para cuando el profesor requiera utilizar dichas herramientas.

Para la realización de reservaciones del equipo de cómputo y aulas los usuarios deberán considerar los siguientes aspectos sin importar si se trata de profesores o alumnos:

* La reservación por parte del alumno se deberá realizar con tres días de anticipación y deberá de comunicárselo al encargado de dicha área, estableciendo un horario y día, así como el software que utilizara teniendo una tolerancia máxima de 15 minutos para llegar, de lo contrario su reservación será anulada y el equipo podrá ser asignado a otro usuario.
* Para los docentes que deseen realizar este tipo de reservación deberán realizarla con 2 días de anticipación estableciendo o indicando con el encargado de los laboratorios el día y hora en que hará uso del equipo de cómputo así como la paquetería que utilizara ya que si no se tiene instalada el encargado de mantenimiento deberá instalarla, deberá proceder de igual manera en la modalidad grupal.

**Capítulo 7** De las prohibiciones

Las siguientes actividades quedan prohibidas para los usuarios:

* No se deberá hacer un mal uso del mobiliario, maltratarlo o realizar alguna actividad que pueda ocasionar daños en mesas, teclado o monitor, si el docente detecta un mal uso deberá reportarlo inmediatamente.
* No se deberán introducir alimentos ni bebidas de ningún tipo a los laboratorios considerando los riesgos que esto representaría.
* No se deberá utilizar el equipo de cómputo para escuchar música u otras distracciones que pudiesen distraer a los usuarios de las aulas contiguas.
* No se deban utilizar las máquinas para la instalación de juegos u otro tipo de software de esta índole.
* El horario de entrada será respetado teniendo como máximo una tolerancia de 15 minutos para cada sesión.
* No se deberán realizar en general tareas de otra índole que no estén relacionadas con el ámbito académico que se esté tratando en el momento de uso.
* No se deban extraer partes del mobiliario, si un usuario es encontrado realizando dicho acto será suspendido temporalmente de los laboratorios, quedando abierta otro tipo de sanción.
* Poseer información o llevar a cabo actividades que conduzcan o puedan conducir al uso no autorizado de información o recursos (computacionales o no) de cualquier institución dentro o fuera del Campus, ya sea por el usuario mismo u otras personas.
* Utilizar los equipos instalados en las salas para desplegar material obsceno o que atente contra los valores que promueve el Instituto.
* Intentar violar las medidas de seguridad implementadas en el sistema operativo.
* Compilar y ejecutar programas de dominio público cuya función sea intentar obtener privilegios mayores a los asignados.
* Enviar mensajes a otros usuarios de manera anónima.
* Conectar, desconectar o mover equipo computacional.
* Introducir memorias USB en los puertos con el fin de extaer información confidencial o no permitida, haciendo mal uso de la información.
* Evitar ejecutar programas maliciosos o cuyo fin sea el robo o extracción de información confidencial.
* No copiar programas cuya licencia sea prohibida.

**Capítulo 8** De las sanciones

Toda violación de este reglamento será reportada de inmediato a los encargados de esta área y de mantenimiento ameritando la suspensión temporal de laboratorios para esa persona, dejando abierta la posibilidad de otras sanciones dependiendo de la gravedad del acto.

**Capítulo 9**  confidencialidad de la información

Toda información almacenada en los equipos de cómputo central y no hecha explícitamente pública, será tratada como confidencial, y se harán todas las adecuaciones posibles por garantizar la privacidad de ésta.

En el caso de los equipos instalados en oficinas, será responsabilidad del usuario a quien fue asignado el tomar las medidas necesarias para proteger su información.

La información administrativa y de administración académica contenida en los equipos del Instituto es privada y confidencial, y sólo deberán tener acceso a ella aquellos usuarios del Instituto que por sus funciones así lo requieran y sean autorizados.

**AUDITORIA FISICA**

**1. Alcance de la Auditoria**

* Organización y cualificación del personal de Seguridad.
* Remodelar el ambiente de trabajo.
* Planes y procedimientos.
* Sistemas técnicos de Seguridad y Protección.

**2. Objetivos**

* Revisión de las políticas y Normas sobre seguridad Física.
* Verificar la seguridad de personal, datos, hardware, software e instalaciones
* Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. ¿Se han adoptado medidas de seguridad en el departamento de Sistemas? | **X** |  |  |
| 2. ¿Existe una persona responsable de la seguridad? | **X** |  |  |
| 3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad? |  | **X** |  |
| 4. ¿Existe personal de vigilancia en la institución? | **X** |  |  |
| 5. ¿Existe una clara definición de funciones entre los puestos clave? |  | **X** |  |
| 6. ¿Se investiga a los vigilantes cuando son contratados directamente? |  | **X** |  |
| 7. ¿Se controla el trabajo fuera de horario? |  | **X** |  |
| 8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas? |  | **X** |  |
| 9. ¿Existe vigilancia en el departamento de cómputo las 24 horas? |  | **X** |  |
| 10. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores? | **X** |  |  |
| 11. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización? | **X** |  |  |
| 12. ¿El Departamento Sistemas y las salas tienen salida al exterior? | **X** |  |  |
| 13. ¿Son controladas las visitas y demostraciones a las salas de cómputo? | **X** |  |  |
| 14. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática? | **X** |  |  |
| 15. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude? |  | **X** |  |
| 16. ¿Se ha adiestrado el personal en el manejo de los extintores? |  | **X** |  |
| 17. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores? | **X** |  |  |
| 18. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego? |  | **X** |  |
| 19. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos? |  | **X** |  |
| 20. ¿Saben que hacer los operadores del departamento de cómputo, encaso de que ocurra una emergencia ocasionado por fuego? | **x** |  |  |
| 21. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)? |  | **X** |  |
| 22. ¿Existe salida de emergencia? | **X** |  |  |
| 23. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen? |  | **X** |  |
| 24. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?  25. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo? |  | **X** |  |
| 26. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe? |  |  | **X** |
| 27. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora? |  | **X** |  |
| 28. ¿Se tienen establecidos procedimientos de actualización a estas copias? |  | **X** |  |
| 29. ¿Existe departamento de auditoría interna en la institución? |  | **X** |  |
| 30. ¿El departamento de Sistemas conoce todos los aspectos de auditoría interna en los sistemas? |  | **X** |  |
| 31. ¿Se cumplen? |  | **X** |  |
| 32. ¿Se auditan los sistemas en operación? |  | **X** |  |

**Auditoria física:**

􀂙 **Para hallar el SI**

32 100%

11 X

**X = 34.375**

􀂙 **Para hallar el NO**

32 100%

20 X

**X = 62.5**

**LISTADO DE VERIFICACION DE AUDITORIA FISICA**

**Gestión Física de Seguridad**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Los objetivos de la instalación física de computo |  | *X* |  |  |  |
| Las características físicas de las salas de sistemas son seguras |  | *X* |  |  |  |
| Los componentes físicos de computo |  |  | *X* |  |  |
| La conexiones de los equipos de las comunicaciones e instalaciones  físicas |  |  | *X* |  |  |
| La infraestructura es |  | *X* |  |  |  |
| El equipos es |  |  | *X* |  |  |
| La distribución de los quipos de computo es |  |  | *X* |  |  |

**Evaluación de análisis física de Cómputo**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Evaluación de la existencia y uso de  normas, resolución base legal para el diseño del centro de cómputo. |  |  | *X* |  |  |
| El cumplimiento de los objetivos fundamentales de la organización para  instalar del centro de cómputo. |  | *X* |  |  |  |
| La forma de repartir los recursos informáticos de la organización |  |  | *X* |  |  |
| La confiabilidad y seguridades el uso de la  información institucional  La satisfacción de las necesidades de  poder computacional de la organización. |  | *X* |  |  |  |
| La solución a identificación del centro de cómputo (apoyó). |  |  | *x* |  |  |

**Análisis de la delimitación la manera en que se cumplen:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| La delimitación espacial, por las dimensiones  físicas. |  |  | *X* |  |  |
| La delimitación tecnológica, por los  requerimientos y conocimientos informáticos. |  |  | *X* |  |  |

**Análisis de la estabilidad y el aprovechamiento de los recursos a para instalar el centro de cómputo.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Análisis de la transparencia del trabajo para los usuarios. |  | *X* |  |  |  |
| La ubicación del centro de computo |  |  | *X* |  |  |
| Los requerimientos de seguridad del centro  de computo |  | *X* |  |  |  |

**Evaluación del diseño según el ámbito**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Análisis del ambiente de trabajo |  | *X* |  |  |  |
| Evaluar el funcionamiento de los equipos |  |  | *X* |  |  |
| El local para el trabajo es |  | *X* |  |  |  |
| Los equipos cuentan con ventilación |  | *X* |  |  |  |
| La iluminación |  |  | *X* |  |  |

**Análisis de la seguridad física**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| La seguridad de los equipos. |  |  | *X* |  |  |
| El estado centro de computo esta |  | *X* |  |  |  |
| Los accesos de salida son |  |  | *X* |  |  |

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria física.

**2. Identificación del Cliente**

Departamento De Sistemas, Salas de Computo

**3. Identificación de la Entidad Auditada**

**Caso de estudio**

**4. Objetivos**

* Verificar la estructura de distribución de los equipos.
* Revisar la correcta utilización de los equipos
* Verificar la condición del centro de cómputo.

**5. Hallazgos Potenciales**

* Falta de presupuesto y personal.
* Falta de un local más amplio.
* No existe un calendario de mantenimiento
* Falta de ventilación.
* Falta de capacitación a los operadores

**6. Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2013 y se ha realizado especialmente **al CITIS en el área de sistemas**  de acuerdo a las normas y demás disposiciones aplicable al efecto.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria Física, se complementa con los objetivos de ésta.

**7. Conclusiones:**

**Colocar cada una de las estrategias propuestas que emanan del análisis FODA.**

**8. Recomendaciones**

* **Reubicación de las salas de Informática**
* **Implantación de equipos de última generación**
* **Implantar equipos de ventilación**
* **Implantar salidas de emergencia.**
* **Elaborar un calendario de mantenimiento de rutina periódico.**
* **Capacitar al personal.**

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 DE AGOSTO AL 30 SEPTIEMBRE** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **16 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
| **VIANNEY DE LOS ANGELES PEREZ GOMEZ** |  |
| **ISAMAR RAMIREZ AZPEITIA** |  |
| **ADOLFO BOTE VAZQUEZ** |  |
| **ALFREDO MACOUZET ORTEGA** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**AUDITORIA DE LA OFIMATICA**

**1. Alcance de la Auditoria.**

* Planes y procedimientos
* Políticas de Mantenimiento
* Inventarios Ofimáticos
* Capacitación del Personal

**2. Objetivos de la Auditoria.**

Realizar un informe de Auditoría con el objeto de verificar la existencia de controles

Preventivos, defectivos y correctivos, así como el cumplimiento de los mismos por los

usuarios.

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. ¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de Computación, incluyendo un estudio costo beneficio? | **X** |  |  |
| 2. ¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación? | **X** |  |  |
| 3. ¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales? |  | **X** |  |
| 4. ¿se cuenta con software de oficina? | **X** |  |  |
| 5. ¿Se han efectuado las acciones necesarias para una mayor participación de proveedores? | **X** |  |  |
| 6. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica? | **X** |  |  |
| 7. ¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado? |  | **X** |  |
| 8. ¿Se han implantado claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado? | **X** |  |  |
| 9. ¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación? |  | **X** |  |
| 10. ¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos? |  | **X** |  |
| 11. ¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos? | **X** |  |  |
| 12. ¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos? |  |  | **X** |
| 13. ¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso? | **X** |  |  |
| 14. ¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.? |  | **X** |  |
| 15. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras entre otras |  | **X** |  |
| 16. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de Variación de voltaje como: reguladores de voltaje, supresores pico, UPS,  generadores de energía? | **X** |  |  |
| 17. ¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación? | **X** |  |  |
| 18. ¿Se han Adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo? | **X** |  |  |
| 19. ¿Si se vence la garantía de mantenimiento del proveedor se contrata mantenimiento preventivo y correctivo? |  | **X** |  |
| 20. ¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos? |  | **X** |  |
| 21. ¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa? |  | **X** |  |
| 22. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos? |  | **X** |  |
| 23. ¿Se propende a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación sobre modificaciones incluidas? |  | **X** |  |
| 24. Existen licencias. | **X** |  |  |

**Auditoria Ofimática**

􀂙 **Para hallar el SI**

24 100%

12 X

**X = 50**

􀂙 **Para hallar el NO**

24 100%

11 X

**X = 45.83**

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria de la Ofimática

**2. Identificación del Cliente**

**3. Identificación de la Entidad Auditada**

**4. Objetivos**

* Verificar si el hardware y software se adquieren siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
* Verificar si la selección de equipos y sistemas de computación es adecuada
* Verificar la existencia de un plan de actividades previo a la instalación
* Verificar que los procesos de compra de Tecnología de Información, deben estar
* sustentados en Políticas, Procedimientos, Reglamentos y Normatividad en General, que aseguren que todo el proceso se realiza en un marco de legalidad y cumpliendo con las verdaderas necesidades de la organización para hoy y el futuro, sin caer en omisiones, excesos o incumplimientos.
* Verificar si existen garantías para proteger la integridad de los recursos informáticos.
* Verificar la utilización adecuada de equipos acorde a planes y objetivos.

**5. Hallazgos Potenciales**

􀂾 No tienen licencias de software.

􀂾 Falta de software de aplicaciones actualizados.

􀂾 No existe un calendario de mantenimiento ofimático.

􀂾 Faltan material ofimática.

􀂾 Falta de presupuesto.

􀂾 Carece de seguridad en Acceso restringido de los equipos ofimáticos y software.

**6. Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2011 y se ha realizado especialmente al

**CASO DE ESTUDIO** de acuerdo a las normas y demás disposiciones aplicable al efecto.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la

auditoria Ofimática, se complementa con los objetivos de ésta.

**7. Conclusiones:**

􀁸 Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar

cada uno de los objetivos contenidos en el programa de auditoría.

􀁸 El Departamento de Sistemas y las salas de cómputo presenta deficiencias sobre el

debido cumplimiento de Normas de seguridad.

􀁸 La escasez de personal debidamente capacitado.

􀁸 Cabe destacar que los sistemas ofimáticos pudiera servir de gran apoyo a la

organización, el cual no es explotado en su totalidad por falta de personal capacitado.

**8. Recomendaciones**

􀁸 Se recomienda contar con sellos y firmas digitales.

􀁸 Un de manual de funciones y roles para cada puesto de trabajo dentro del área.

􀁸 Reactualización de datos.

􀁸 Adquisición de Licencias.

􀁸 Implantación de equipos de última generación.

􀁸 Elaborar un calendario de mantenimiento de rutina periódico.

􀁸 Capacitar al personal.

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 DE AGOSTO AL 30 SEPTIEMBRE** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **16 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
| **VIANNEY DE LOS ANGELES PEREZ GOMEZ** |  |
| **ISAMAR RAMIREZ AZPEITIA** |  |
| **ADOLFO BOTE VAZQUEZ** |  |
| **ALFREDO MACOUZET ORTEGA** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**AUDITORIA A LOS SISTEMAS DE REDES**

**1. Alcance de la Auditoria.**

􀂾 Calificación del personal

􀂾 Sistemas técnicos de la red

􀂾 Mantenimiento de la Red

**2. Objetivos de la Auditoria.**

Realizar un informe de Auditoría con el objeto de verificar la adecuación de las medidas

aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

**3. Referencia Legal.**

􀁸 Manual de Autoprotección aprobado por O.M. de 29/11/84, NBE-CPI 96 (RD 2177/96).

**4. Resultados.**

Se obtendrá:

􀁸 Informe de Auditoría detectando deficiencias en el Sistema de Redes.

􀁸 Plan de recomendaciones a aplicar en función de:

o Normativa a cumplir

o Recomendaciones

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. El departamento de Sistemas tiene una política definida de planeamiento de tecnología de red? | **X** |  |  |
| 2. Esta política es acorde con el plan de calidad de la organización? | **X** |  |  |
| 3. El departamento de Sistemas tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios tecnológicos o en la organización? | **X** |  |  |
| 4. Existe un inventario de equipos y software asociados a las redes de Datos? | **X** |  |  |
| 5. Las redes de Datos se encuentran certificadas? | **X** |  |  |
| 6. Existe un plan de infraestructura de redes? | **X** |  |  |
| 7. El plan de compras de hardware y software para el sector redes está de acuerdo con el plan de infraestructura de redes? |  | **X** |  |
| 8. La responsabilidad operativa de las redes está separada de las de operaciones del computador? |  | **X** |  |
| 9. Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados | **X** |  |  |
| 10. Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas? |  | **X** |  |
| 11. Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red? |  | **x** |  |
| 12. Existen protocolos de comunicaron establecida | **X** |  |  |
| 13. Existe una topología estandarizada en toda la organización | **X** |  |  |
| 14. Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes?  15. ¿La transmisión de la información en las redes es segura? |  | **X** |  |
| 16. ¿El acceso a la red Wi-fi tiene password? | **X** |  |  |

**Auditoria de Redes:**

􀂙 **Para hallar el SI**

16 100%

10 X

**X = 62.5**

􀂙 **Para hallar el NO**

16 100%

6 X

**X = 37.5**

**AREA CRITICA REDES**

LISTADO DE VERIFICACIÓN DE AUDITORIA DE REDES

**Gestión Administrativa de la red.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Los objetivos de la red de computo |  | *X* |  |  |  |
| Las características de la Red de computo |  | *X* |  |  |  |
| Los componentes físicos de la red de Computo |  | *X* |  |  |  |
| La conectividad y las Comunicaciones de la  red de computo |  |  | *X* |  |  |
| Los servicios que Proporcionan La red de  computo |  |  | *X* |  |  |
| Las configuraciones, topologías , tipos  Y cobertura de las redes de cómputo. |  | *X* |  |  |  |
| Los protocolos de Comunicación interna  de la red. |  |  | *X* |  |  |
| La administración de la red de Cómputo. |  |  | *X* |  |  |
| La seguridad de las redes de cómputo |  |  | *X* |  |  |

**Evaluación De Análisis De La Red De Cómputo**

Evaluar y calificar el cumplimiento de los siguientes aspectos:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Evaluación de la existencia y uso de  metodologías, normas, estándares y  políticas para el análisis y diseño de redes  de cómputo. |  | *X* |  |  |  |
| Análisis de la definición de la problemática y  solución para instalar redes de cómputo en  la empresa. |  |  | *X* |  |  |
| Análisis de cumplimiento de los objetivos  fundamentales de la organización para  instalar una red de cómputo, evaluando en  cada caso. |  |  | *X* |  |  |
| La forma de repartir los recursos  informáticos de la organización,  especialmente la información y los activos |  |  | *X* |  |  |
| La cobertura de servicios informáticos para  la captura, el procesamiento y la emisión de  información en la organización |  |  | *X* |  |  |
| La cobertura de los servicios de comunicación. |  |  | *X* |  |  |
| La frecuencia con que los usuarios recurren  a los recursos de la red |  | *X* |  |  |  |
| La confiabilidad y seguridades el uso de la  información institucional. |  | *X* |  |  |  |
| La centralización , administración, operación  asignación y el control de los recursos informáticos de la organización. |  | *x* |  |  |  |
| La distribución equitativa de los costos de  adquisición y el control de los recursos  informáticos de la organización. |  |  | *X* |  |  |
| La escalabilidad y migración de los recursos  computacionales de la organización. |  |  | *X* |  |  |
| La satisfacción de las necesidades de poder  computacional de la organización ,sea con  redes ,cliente /servidor o mainframe |  |  | *X* |  |  |
| La solución a los problemas de  comunicación de información y datos en las  áreas de la organización |  | *X* |  |  |  |

**Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa:**

**Evaluar y calificar el cumplimiento de los siguientes aspectos**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| El estudio de factibilidad tecnológica |  | *X* |  |  |  |
| El estudio factibilidad económica |  |  | *X* |  |  |
| El estudio de factibilidad administrativa |  |  | *X* |  |  |
| El estudio de factibilidad operativa |  |  | *x* |  |  |

**Evaluación del diseño e implementación de la red según el ámbito de cobertura.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Análisis de las redes de multi-computadoras |  |  | *X* |  |  |
| Evaluar el funcionamiento de la cobertura de punto a punto |  |  | *X* |  |  |
| Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas |  | *X* |  |  |  |
| Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes |  |  | *X* |  |  |

**Análisis de la red de área local (L A N).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***CRITERIO*** | ***100% EXCELENTE*** | ***80%***  ***BUENA*** | ***60% REGULAR*** | ***40%***  ***MINIMO*** | ***20%***  ***NO CUMPLE*** |
| Evaluar el uso adecuado y confiable de la  tecnología utilizada internamente para la  transmisión de datos |  |  | *X* |  |  |
| Evaluar la Restricción adoptada para  establecer el tamaño de la red |  | *X* |  |  |  |
| Evaluar la velocidad. |  |  | *X* |  |  |

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria del Sistema de Redes

**2. Identificación del Cliente**

Departamento De Sistemas, Salas de Computo

**3. Identificación de la Entidad Auditada**

**4. Objetivos**

􀂾 Evaluar el tipo de red, arquitectura topología, protocolos de comunicación, las conexiones,

accesos privilegios, administración y demás aspectos que repercuten en su instalación.

􀂾 Revisión del software institucional para la administración de la red.

**5. Hallazgos Potenciales**

􀁸 No se cuenta con un Software que permita la seguridad de restricción y/o control a la Red.

􀁸 No existe un plan que asegure acciones correctivas asociadas a la conexión con redes

externas.

􀁸 No están definidos los parámetros o normas de calidad.

􀁸 El departamento de Sistemas no tiene un plan que permite modificar en forma oportuna el

plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios

tecnológicos.

􀁸 No existe un calendario de mantenimiento de rutina periódico del hardware definido por el

Departamento de Sistemas.

􀁸 No existe un plan proactivo de tareas a fin de anticipar los problemas y solucionarlos antes

de que los mismos afecten el desempeño de la red

**6. Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2011 y se ha realizado especialmente al

área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

**7. Conclusiones:**

􀁸 Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada

uno de los objetivos contenidos en el programa de auditoría.

􀁸 El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de

Normas de redes y funciones.

**8. Recomendaciones**

􀁸 Elaborar toda la documentación técnica correspondiente a los sistemas de redes.

􀁸 Evaluar e implementar un software que permita mantener el resguardo de acceso de los

archivos de programas.

􀁸 Implementar un plan que permita modificar en forma oportuna el plan a largo plazo de

tecnología de redes.

􀁸 Elaborar un calendario de mantenimiento de rutina periódico del hardware.

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 DE AGOSTO AL 30 SEPTIEMBRE** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **16 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
| **VIANNEY DE LOS ANGELES PEREZ GOMEZ** |  |
| **ISAMAR RAMIREZ AZPEITIA** |  |
| **ADOLFO BOTE VAZQUEZ** |  |
| **ALFREDO MACOUZET ORTEGA** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**BALANCE DE RESULTADOS**

|  |  |  |
| --- | --- | --- |
| **AUDITORIA** | **SI** | **NO** |
| **FISICA** |  | **X** |
| **OFIMATICA** | **X** |  |
| **REDES** | **X** |  |

**CONCLUSIONES**

La principal conclusión a la que hemos podido llegar, es que toda empresa, pública o privada, que posean Sistemas de Información medianamente complejos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Hoy en día, el 90 por ciento de las empresas tienen toda su información estructurada en Sistemas Informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente. La empresa hoy, debe/precisa informatizarse.

El éxito de una empresa depende de la eficiencia de sus sistemas de información. Una empresa puede tener un staff de gente de primera, pero tiene un sistema informático propenso a errores, lento, vulnerable e inestable; si no hay un balance entre estas dos cosas, la empresa nunca saldrá a adelante. En cuanto al trabajo de la auditoria en sí, podemos remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoria de Sistemas debe hacerse por gente altamente capacitada, una auditoria mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.

**INFORME FINAL DE AUDITORIA**

**La presente Auditoría ha sido solicitada por la Alta Dirección, quien aprobó los objetivos y alcance de la misma. Por lo anterior, se reconoce a ésta como cliente de la misma.**

**Objetivos**

* **Verificar la eficacia y eficiencia de los procesos y procedimientos asociados a las actividades diariamente realizadas por el personal participante.**
* **Localizar las oportunidades de mejora, para algunos procesos.**

**¿Cómo se auditó?**

* **Con la participación de los auditores Adolfo Bote Vazquez, Isamar Ramirez Azpeitia, Alfredo Macouzet Ortega y como auditor líder Vianney de los Angeles Perez Gomez.**
* **Mediante entrevistas, encuestas y revisión documental se verificó el cumplimiento de los criterios de la auditoría en los procesos y áreas bajo alcance de la misma.**

**RESULTADOS**

* CITIS cuenta con la siguiente documentación:
* Carece de la siguiente información
* De la información que se careceré, se elaborara y se implementara de la siguiente forma:

|  |  |  |  |
| --- | --- | --- | --- |
| TIPO DE DOCUMENTO | RESPONSABLE | FECHA ESTIMADA ELABORACION | FECHA ESTIMADA DE IMPLEMENTACIÓN |
| PLAN DE CONTINGENCIA EN CASO DE DESASTRES | DIRECTOR DEL CITIS | 6 MESES | 1 AÑO |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* El personal entrevistado demostró interés en trabajar utilizando las normas de Auditoria correspondientes.
* El personal mostró interés en iniciar los trabajos para evaluar el desempeño de sus procesos, en seguir otorgando los servicios y productos que por su experiencia está comprometido a realizar.
* Se confirma el compromiso y la oportunidad de avanzar hacia la mejora continua en la organización.
* La Alta Dirección tiene identificado los Objetivos de Calidad e indicadores institucionales.

**RESUMEN DE NO CONFORMIDADES**

|  |  |  |
| --- | --- | --- |
| **NO.** | **TIPO DE HALLAZGO** | **DESCRIPCIÓN DEL HALLAZGO** |
| 1 | **No Conformidad Mayor:**  **No hay o no se conocen los criterios para análisis medición y seguimiento de los resultados y operación de Procesos. REINCIDENTE EN LA AU-O4 PUNTO 7.5 DE LA NORMA** | * No se cuenta con la bitácora de entradas y salidas del lugar * No se da el mantenimiento establecido para el lugar, y no se siguen la mayoría de manuales de operación y de instrucciones. |

**ÁREAS DE OPORTUNIDAD O DE MEJORA**

EN BASE A LAS AUDITORIAS ARRIBA REALIZADAS PLANTEAR LAS OPORTUNIDADES DE MEJORA.