AUDITORIA DE SISTEMAS

****

**AUDITORIA SALAS DE SISTEMAS**

**Pika and friends**

**AUDITORES**

**Hernández Montes Ignacio**

**Gómez Rueda Luis Alberto**

**Picazo Hernández Francisco Javier**

**INTRODUCCIÓN**

A finales del siglo XX, los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los sistemas de información de la empresa.

La informática hoy, esta subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informativos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el “management” o gestión de la empresa. Cabe aclarar que la informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoria informática.

El término de auditoria se ha empleado incorrectamente con frecuencia ya que se ha considerado, como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase “tiene auditoria” como sinónimo de que, en dicha entidad, antes de, realizarse la auditoria, ya se habían detectado fallas.

**INDICE DEL PROYECTO DE AUDITORIA DE SISTEMAS**

Contenido

[Capítulo I INVESTIGACIÓN PRELIMINAR 7](#_Toc371981160)

[Objetivos a corto y largo plazo. 7](#_Toc371981161)

[RECURSOS MATERIALES Y TECNICOS 8](#_Toc371981162)

[Manual de formas. 10](#_Toc371981163)

[ Manual de procedimientos de los sistemas 11](#_Toc371981164)

[PERSONAL PARTICIPANTE 13](#_Toc371981165)

[Capítulo II Auditoría Informática 16](#_Toc371981166)

[Institución: 16](#_Toc371981167)

[Logo: 16](#_Toc371981168)

[Eslogan: 16](#_Toc371981169)

[Dirección: 16](#_Toc371981170)

[1.2.Servicios que brinda: 18](#_Toc371981171)

[1.3ÁREA INFORMÁTICA. 18](#_Toc371981172)

[AUDITORIA DE SISTEMAS 18](#_Toc371981173)

[1.5. OBJETIVOS Y ALCANCE 18](#_Toc371981174)

[1.6. ENFOQUE A UTILIZAR 19](#_Toc371981175)

[1.7. DOCUMENTOS A SOLICITAR 19](#_Toc371981176)

[1.8. ORGANIGRAMA 20](#_Toc371981177)

[1.9. RELACION DE FUNCIONARIOS DEL AREA A EXAMINAR 20](#_Toc371981178)

[1.10. TIPO DE SOFTWARE A UTILIZAR 20](#_Toc371981179)

[3. PUNTOS DEBILES Y AMENAZAS. 28](#_Toc371981180)

[**MATRIZ FODA(PROPUESTA)** 28](#_Toc371981181)

[4.1. PUNTOS DÉBILES Y AMENAZAS. 29](#_Toc371981182)

[4.2. RECOMENDACIONES 29](#_Toc371981183)

[5. CABLEADO ESTRUCTURADO. 29](#_Toc371981184)

[NORMA TIA/EIA-568-B 29](#_Toc371981185)

[Objetivos 29](#_Toc371981186)

[5.1. PUNTOS DÉBILES Y AMENAZAS. 30](#_Toc371981187)

[5.2. RECOMENDACIONES 30](#_Toc371981188)

[6. CONEXIONES DE REDES 30](#_Toc371981189)

[6.1. PUNTOS DÉBILES Y AMENAZAS 30](#_Toc371981190)

[7. LICENCIAMIENTO DEL SOFTWARE 30](#_Toc371981191)

[7.2. PLANES DE CONTINGENCIA. 31](#_Toc371981192)

[7.2.1. PUNTOS DÉBILES Y AMENAZAS. 31](#_Toc371981193)

[7.3. NORMAS PARA USO DE LAS SALAS DE SISTEMAS 31](#_Toc371981194)

[Planeación de la auditoría 36](#_Toc371981195)

[CONTROLES 36](#_Toc371981196)

[CONTROL DE OPERACIÓN 40](#_Toc371981197)

[CONTROLES DE SALIDA 45](#_Toc371981198)

[CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO 45](#_Toc371981199)

[CONTROL DE ALMACENAMIENTO MASIVO 46](#_Toc371981200)

[CONTROL DE MANTENIMIENTO 49](#_Toc371981201)

[ORDEN EN EL CENTRO DE CÓMPUTO 50](#_Toc371981202)

[1.5.- MODELOS DE CONTROL 51](#_Toc371981203)

[CONCLUSIONES 72](#_Toc371981204)

# Capítulo I INVESTIGACIÓN PRELIMINAR

**ADMINISTRACIÓN**

En el área de informática, se cuenta con 21 equipos, un site y un equipo para mantener el aire acondicionado. La encargada del área de sistemas, es quien le da a conocer a cada uno de los integrantes de ésta área el orden que tiene que seguir para poder llevar a cabo un desempeño más óptimo a la hora de que cada uno realice sus actividades.

**A NIVEL DEL ÁREA DE INFORMÁTICA**

# Objetivos a corto y largo plazo.

No tienen, como tal en el área de informática. A nivel institución:

**Misión.**

Tiene como misión contribuir al progreso de la sociedad hidalguense a través de un ejercicio periodístico libre, veraz, crítico y oportuno. Edita, publica y produce información de carácter político, económico, social, cultural y deportivo, comprometido con la veracidad y certidumbre de la noticia, desde su generación hasta la distribución vía sus alternativas impresas y de Internet. Generar productos de elevada calidad que dejen entre los lectores la certeza de estar bien informados para triunfar en su empleo y vida diaria. Ser una empresa socialmente responsable involucrada en la superación profesional y personal de sus empleados. A partir de la premisa de que la veracidad y los recursos humanos son los principales activos de un medio de comunicación, con estándares de excelencia crea valor duradero para los recursos de la compañía a través de la inversión y la persistencia en el esfuerzo.

**Visión**

Es  referente en el periodismo hidalguense, su publicación se destaca por su credibilidad y certidumbre que dan al lector poder de opinión. El Independiente de Hidalgo es un factor que influye en la opinión pública.

**Propuesta:**

Objetivos a corto plazo:

El departamento de sistemas, tiene como objetivo poder mantener en óptimas condiciones todos los equipos para poder que se puedan realizar de forma óptima todas las actividades que se llevan a cabo dentro de la empresa

*Objetivos a largo plazo.*

Seguir manteniendo la efectividad mostrada durante los últimos años, obteniendo en su mayor capacidad los equipos, además de darles un óptimo mantenimiento cada cierto periodo de tiempo.

# RECURSOS MATERIALES Y TECNICOS

Estudios de viabilidad.

Este estudio tiene como fin, conocer si se cuenta con la viabilidad necesaria para que la auditoría que se realiza, se muestre que cada uno de los elementos que integran esta unidad, son capaces de poder realizar de forma óptima sus actividades encomendadas, de la forma más eficiente posible.

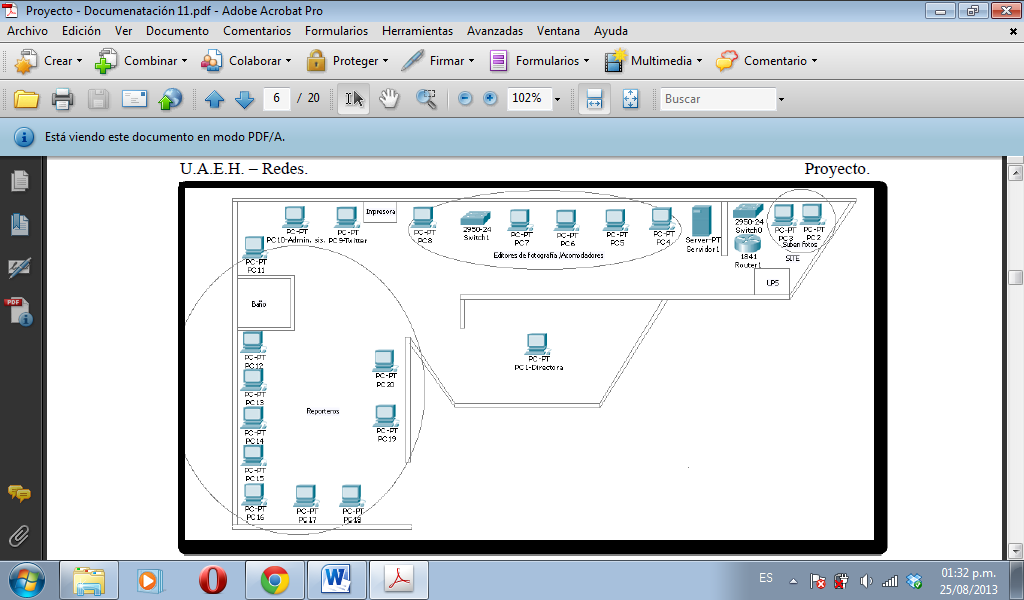
Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)

Se cuenta con 21 equipos, de los cuáles, 16 son marca Dell modelo studio Z con 512 mb de memoria para videos, 2GB de RAM y 160 GB de disco duro.

5 equipos MAC con 750 GB de disco duro, 8GB de RAM, procesador a 2.9 GHZ.

El servidor cuenta con 1 procesador XEON a 3.2 Ghz, 1GB de RAM y 4 discos duros de 120 GB.

UBICACIÓN:



Fechas de instalación de los equipos y planes de instalación.

Los equipos fueron instalados en el mayo del 2011 y, fueron configurados con una red tipo estrella para poder mantener conectada en red la institución y así poder mantenerse conectados unas computadoras con otras para el manejo de la información.

Contratos vigentes de compra, renta y servicio de mantenimiento.

No cuentan con contratos de mantenimiento, debido a que uno de los encargados del área de sistemas, es el encargado de darle el mantenimiento a cada uno de los equipos con los que se cuentan.

Contratos de seguros.

No cuentan.

Convenios que se tienen con otras instalaciones.

No tienen

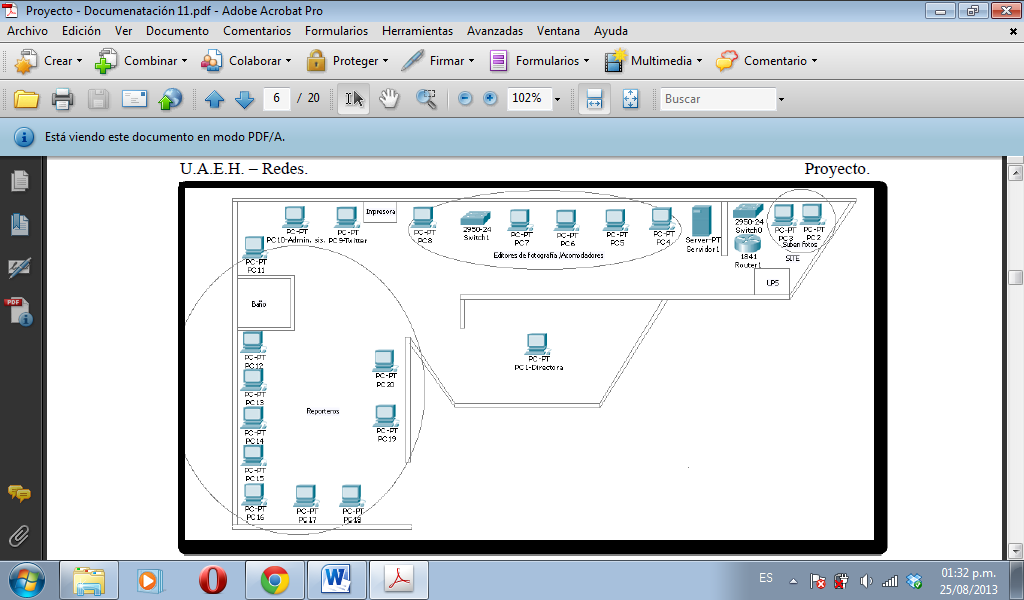
Configuración de los equipos y capacidades actuales y máximas.

Los equipos actualmente tienen una configuración básica, dado que para lo que se necesita, sólo es necesario que tengan acceso a internet, y el uso básico de la paquetería de office, esto para los reporteros y correctores, el encargado de sistemas, diseñadores y paginadores, necesitan de equipos con capacidades un poco más potentes, por ello utilizan equipos MAC, debido a los programas que utilizan, facilitando la arquitectura de éstos equipos, para su óptimo desempeño dentro de la empresa.

Planes de expansión.

No tienen

Ubicación general de los equipos.



Políticas de operación.

No tienen de forma escrita, pero si tienen en claro, que el centro opera con ciertas políticas, como lo son el pasar notas con la inicial del nombre del reportero, imprimir sus guías para que los paginadores puedan ir contemplando el espacio que van a usar para la nota.

Políticas de uso de los equipos.

Los usuarios, tienen prohibido ingresar a redes sociales como facebook, twitter, youtube, esto porque además de mermar un poco en el tiempo de realización de sus actividades, reducen el ancho de banda, el cuál es muy necesario que este hasta su máxima capacidad, debido a que las actividades realizadas en esta empresa no tienen contratado un paquete de banda ancha grande.

# Manual de formas.

El procedimiento que se maneja en el área de sistemas respecto a la información que se maneja, es la siguiente:

El reportero una vez que ha terminado de realizar su nota, la guarda con la inicial de su nombre y el nombre que llevará la nota.

El reportero tiene que mostrar un avance de sus notas del día que va a publicar, para que los paginadores y la encargada del área de fotografía pueda buscar fotos que ilustren la nota, y ésta guía también se le da a los paginadores, para que vayan diseñando el espacio que se le dará a la nota en la hoja del periódico.

La encargada de fotografía una vez que ha encontrado la foto ilustrativa, la edita y la adapta al espacio en que será impresa en la hoja del periódico y se la pasa a los paginadores.

Los paginadores una vez que han armado la página con las notas, anuncios y fotos que llevará cada página, se encargan de imprimir cada hoja, mostrando cómo quedará cada página que formará el periódico y le mandan el archivo a la encargada de sistemas, para que vaya almacenando cada nota en la base de datos del periódico.

La encargada de sistemas, le manda estas notas a la otra persona encargada de sistemas, quien se encarga de subir y programar cada nota para que sea mostrada en la página web del periódico, además también se encarga de hacer con estas notas la versión digital del periódico.

1. Manual de procedimientos de los sistemas. No tiene, pero proponemos:

Logotipo:



Nombre oficial de la institución: El independiente de Hidalgo.

Introducción: El presente manual, permite conocer a detalle el funcionamiento de esta unidad. Permitiendo conocer el funcionamiento interno, auxiliando en la capacitación del personal, ya que se describe detalladamente las actividades de cada puesto.

Objetivos de los procedimientos:

Conocer el funcionamiento interno, con base a conocer cada actividad que realizan todos y cada uno de los elementos que integran ésta organización para su óptimo desempeño.

Descripción genérica.

A Grosso modo, la forma en la que opera esta institución es:

Creación de la nota por parte de los reporteros.

El encargado de la sección de internacional, se encarga de buscar a través de las páginas de internet, las noticias más relevantes durante el día, para después ser seleccionadas y que así sean publicadas en el medio.

Los corresponsales mandan sus notas a uno de los reporteros para que las selecciones y le sean pasado los avances a los correctores y después a los paginadores.

Se imprimen las guías que contienen las notas que serán publicadas, para que los paginadores y la persona encargada de fotografía busque las imágenes que puedan ilustrar la nota.

La directora del periódico ha armado la guía de cómo se armará el periódico. Esta guía se pasa al encargado del área de sistemas

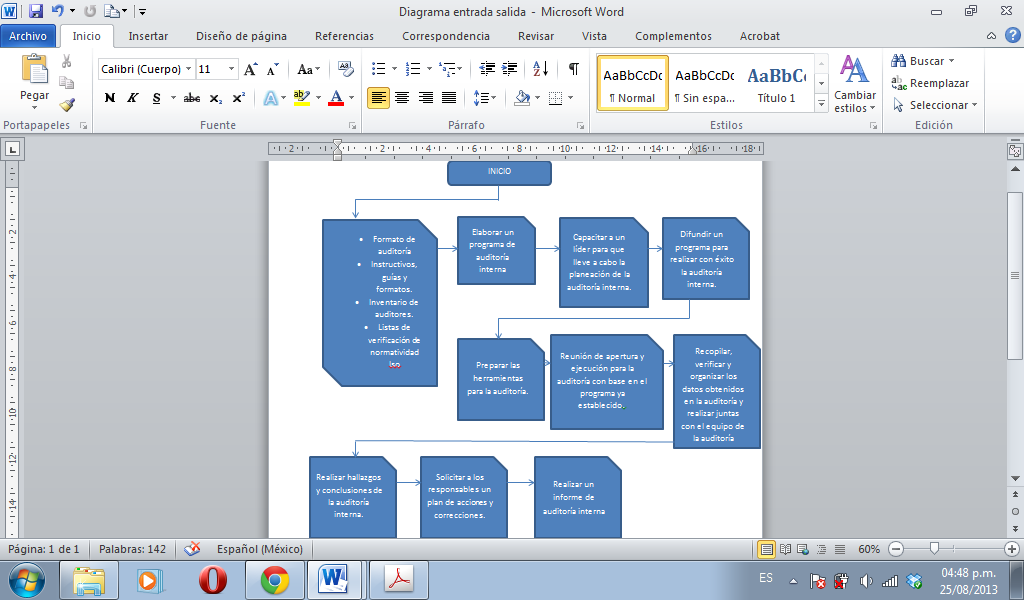
La persona encargada de fotografía, manda la imagen con la que se ilustrará la nota a los paginadores

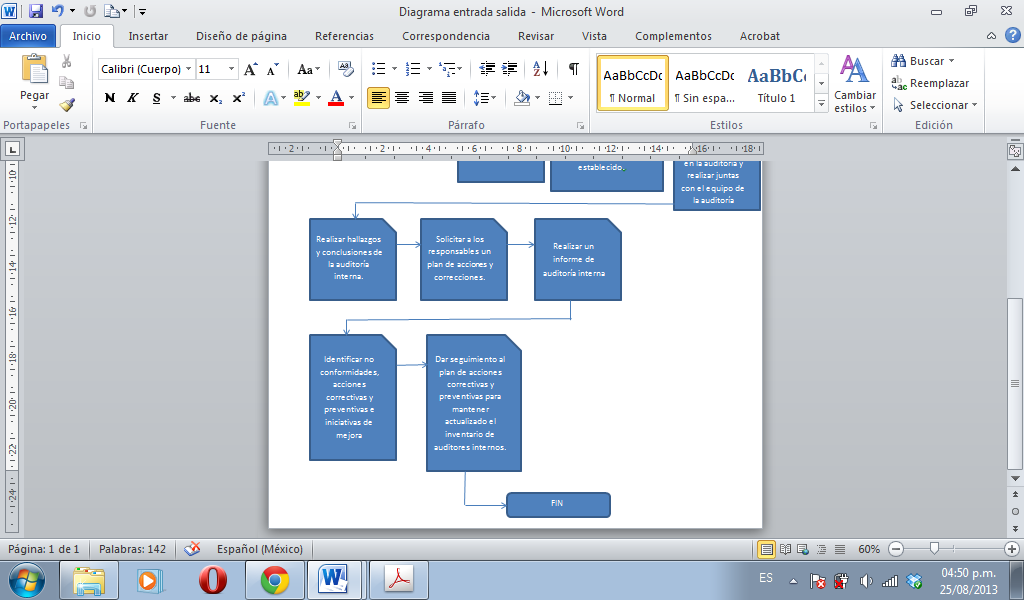
Los paginadores una vez que han recibido las guías, colocan la nota en la hoja del periódico junto con los anuncios y las imágenes que llevará cada página.

Los paginadores pasan las páginas del formato final al encargado de sistemas, para que guarde las notas.

La encargada de sistemas, pasa éstos archivos a otra persona de sistemas, para que suba las notas finales a la página web y también cree la versión digital del periódico.

Diagramas de entrada, archivos, salida.





Fecha de instalación de los sistemas.

Mayo del 2011

Proyecto de instalación de nuevos sistemas.

Por el momento no se tiene planeado instalar nuevos sistemas.

# PERSONAL PARTICIPANTE

El personal encargado de llevar a cabo la auditoría informática, cumple con el siguiente perfil:

Puesto: Auditor Junior

Estudios: 9no semestre de la carrera Licenciatura en Sistemas Computacionales.

Experiencia: Elaboración de diversos proyectos para realización de sistemas de puntos de ventas, creación de páginas web y mantenimiento.

Competencias: Análisis de sistemas, office avanzado, y administración de proyectos, ubuntu.

Buena presentación

Sueldo: 9500 y prestaciones de ley.

Puesto: Auditor Junior

Estudios: 9no semestre de la carrera Licenciatura en Sistemas Computacionales.

Experiencia: Elaboración de diversos proyectos para realización de sistemas de puntos de ventas.

Competencias: Análisis de sistemas, office avanzado, redes y administración de proyectos, redes y Linux.

Buena presentación

Sueldo: 9500 y prestaciones de ley.

El personal que colaboró con la auditoría informática, cumple con el siguiente perfil:

Puesto: Reportero

Estudios: Licenciado en Comunicación.

Experiencia: 6 meses como reportero en periódico el Independiente

Competencias: Análisis acerca de finanzas.

Buena presentación

Sueldo: 1500 y prestaciones de ley.

Puesto: Encargada de Sistemas

Estudios: Licenciado en Sistemas Computacionales.

Experiencia: 3 años como jefa de área de sistemas en el periódico el Independiente. 2 años encargada de darle mantenimiento a servidores.

Competencias: Creación y mantenimiento de servidores, mantenimiento de cómputo.

Buena presentación

Sueldo: 7500 y prestaciones de ley.

Puesto: Corrector

Estudios: Licenciado en Comunicación.

Experiencia: 6 meses como reportero en periódico el Independiente

Competencias: Escritura de reportajes enfocados a los deportes, buena ortografía, facilidad para escribir.

Buena presentación

Sueldo: 1500 y prestaciones de ley.

Puesto: Paginador

Estudios: Licenciado en Diseño Gráfico.

Experiencia: Editor por 3 años de una revista, 3 años como paginador y corrector del periódico Criterio.

Competencias:Manejo de photoshop, indesign.

Buena presentación

Sueldo: 5500 y prestaciones de ley.

# Capítulo II Auditoría Informática

# Institución:

El independiente de Hidalgo

# Logo:

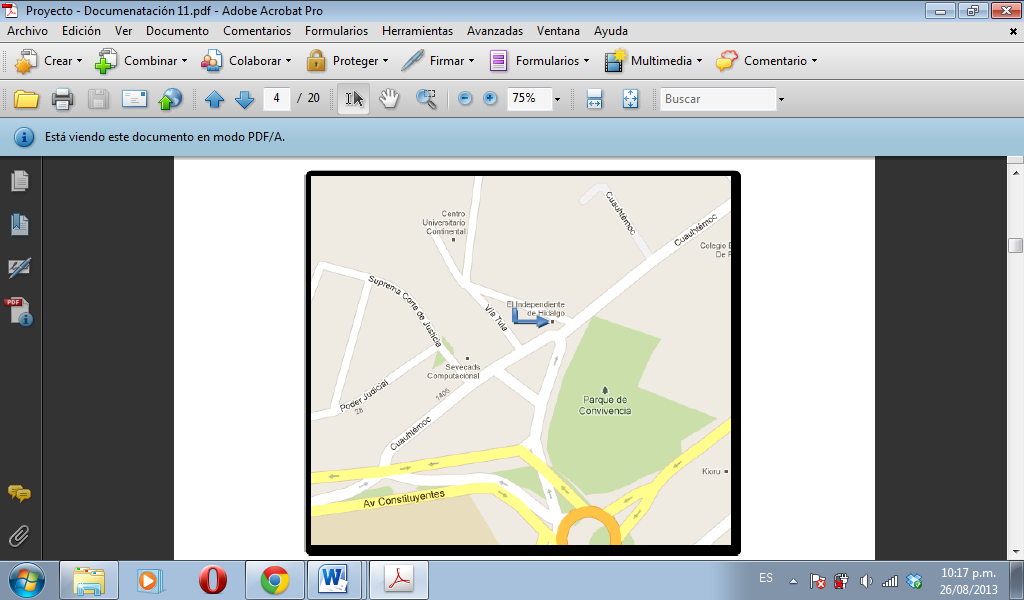


# Eslogan:

**Libre por convicción**

Dirección:calle Cuauhtémoc, esquina con calle República de Salvador, número 1400, C.P. 42060, Pachuca de Soto, Hidalgo.

Ubicación:



Reseña Historica:

15 de abril de 2009 nace el independiente de Hidalgo, de la mano de su casa editorial la voz del aire

Web Site:[http://www.elindependientedehidalgo.com.mx](http://www.elindependientedehidalgo.com.mx/)

Filosofia Institucional:

En el independiente primero son las personas, en ese tenor nos comprometemos con nuestros lectores, anunciantes, trabajadores

y accionistas a laborar todos los días bajo las premisas de velar por la verdad, los valores humanos, la ética y el bien común, por encima de intereses individuales, en un marco de máxima calidad y clara responsabilidad. El independiente se compromete con sus trabajadores al ofrecerles un empleo bien remunerado y acorde con su desempeño y responsabilidades, respetando sus derechos laborales, humanos y ciudadanos. La opinión de los articulistas no refleja la línea editorial de . En apego al derecho de la información este diario abre sus páginas a todas las corrientes ideológicas para que se expresen.

# 1.2.Servicios que brinda:

Edita, publica y produce información de carácter político, social, cultural y deportivo, distribuypendolo por medio de alternativas impresas y de internet.

# 1.3ÁREA INFORMÁTICA.

El área de sistemas esta conformada por una red de tipo estrella, mediante la cuál se comparte la información de los reporteros, con los correctores, los paginadores y fotografía. En total son 21 equipos de cómputo, todos de escritorio, de los cuáles 5 son equipos MAC ocupados por los trabajadores de diseño y paginación.

# 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 de 2013 en el periódico El Independiente de Hidalgo, 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 un mejor desempeño por parte de todo el personal que aquí labora, buscando obtener un mejor desempeño en el área.

1.5.2 OBJETIVOS ESPECIFICOS

Verificación del sistema eléctrico del área 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 realizara en el Independiente de Hidalgo**,**  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

# 1.9. RELACION DE FUNCIONARIOS DEL AREA A EXAMINAR

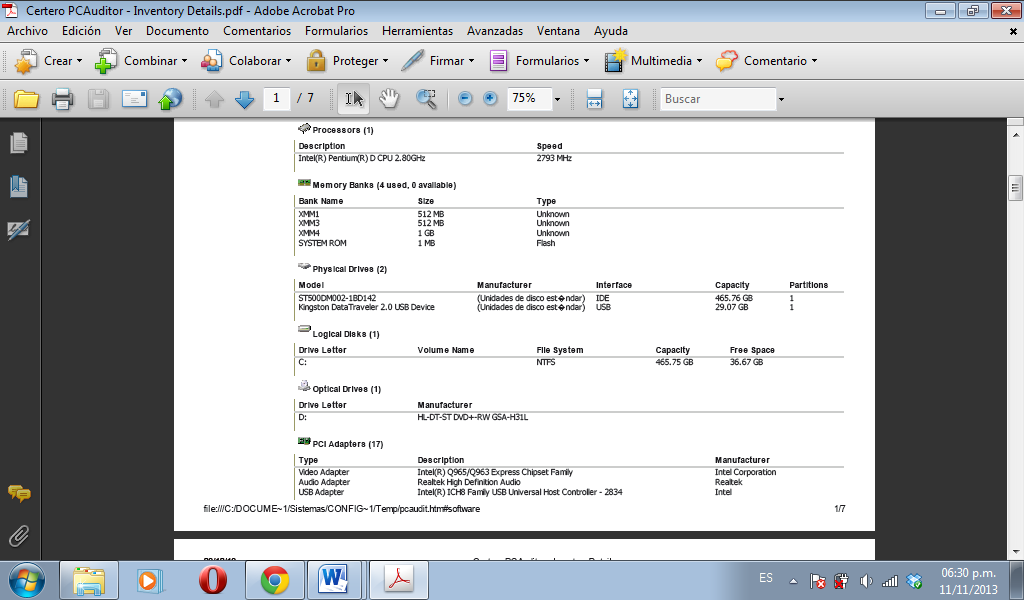
Se relacionaran las personas que tienen relación con el Departamento de Sistemas de Acuerdo lo expresa el organigrama, teniendo en cuenta su cargo.

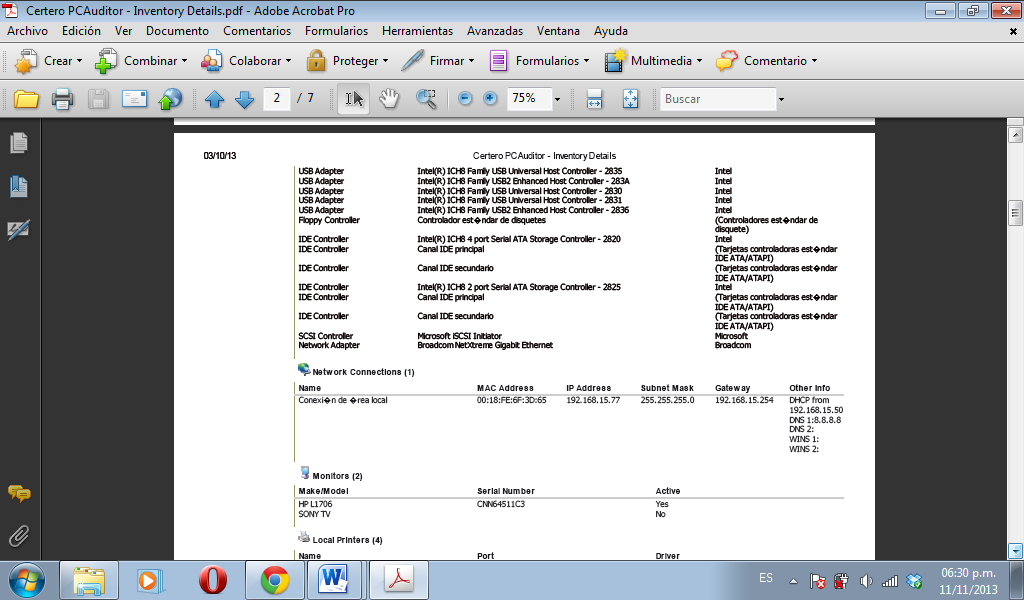
# 1.10. TIPO DE SOFTWARE A UTILIZAR

Se detallara el software utilizado para la verificación de licenciamiento del Software instalado en cada PC.

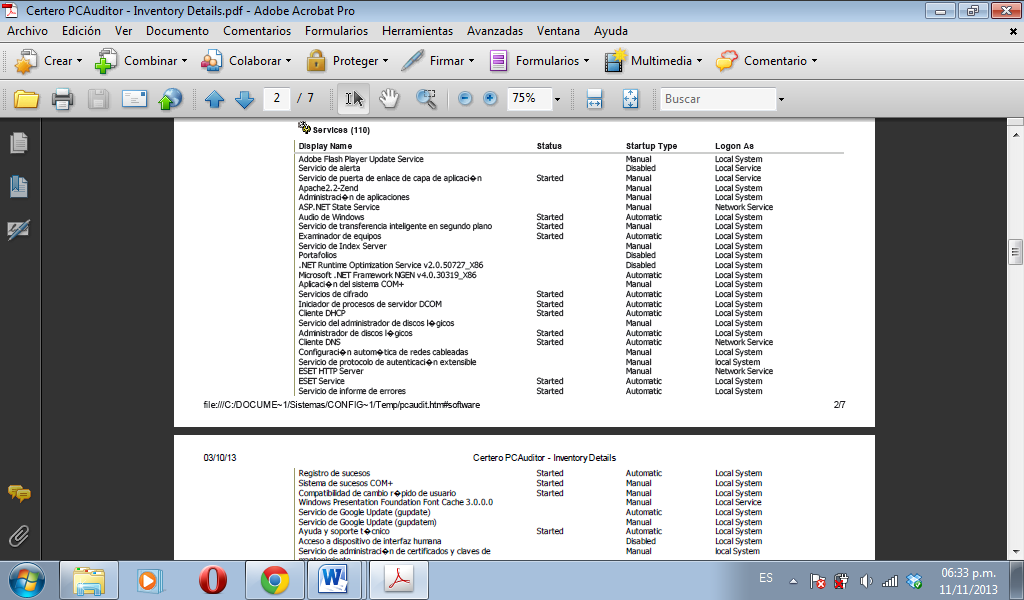
1.7.1 CERTERO PCAUDITOR

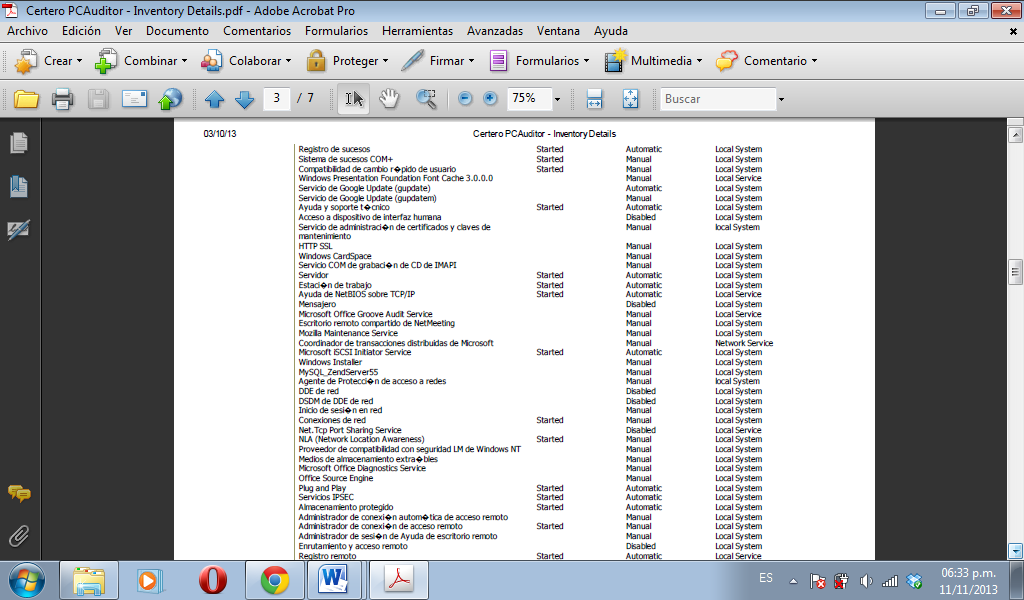
**HARDWARE**

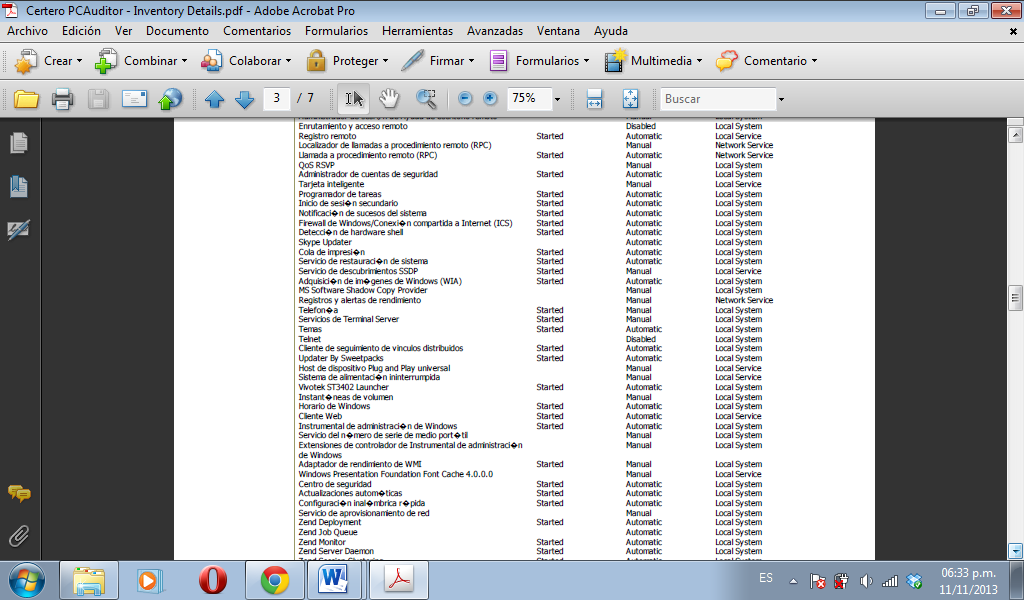




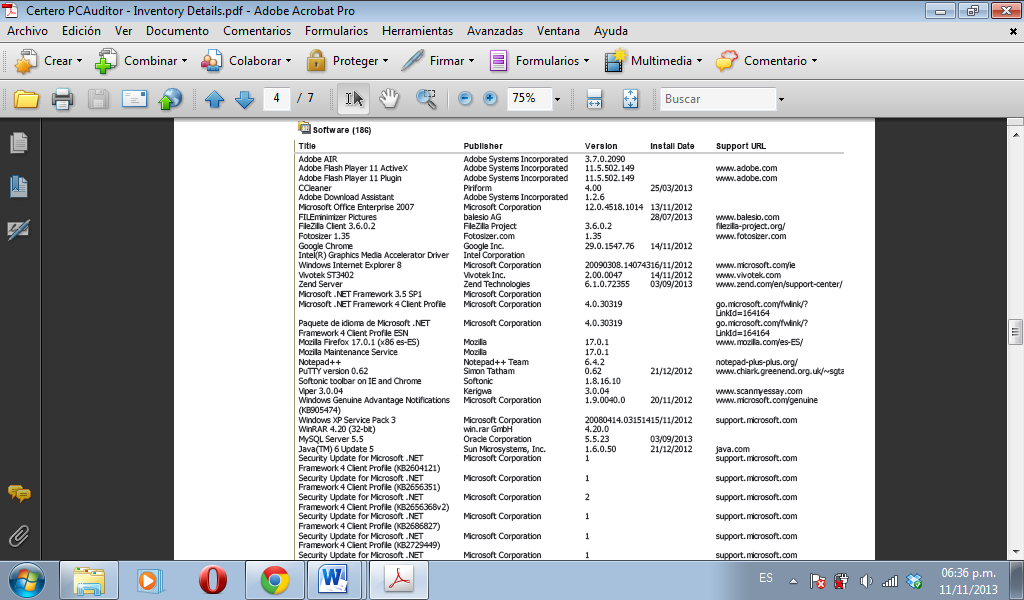
**SERVICES**

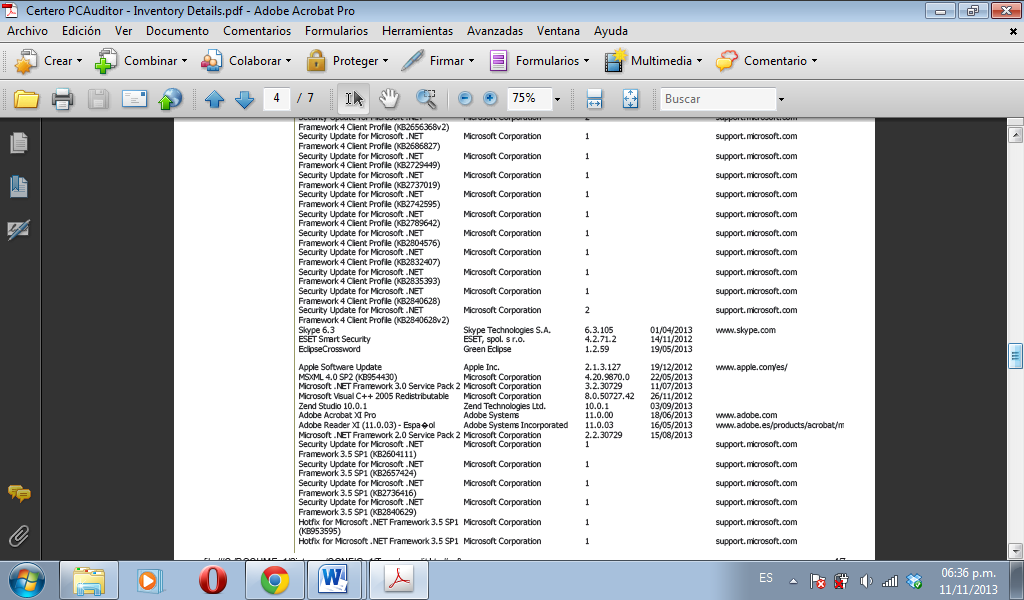




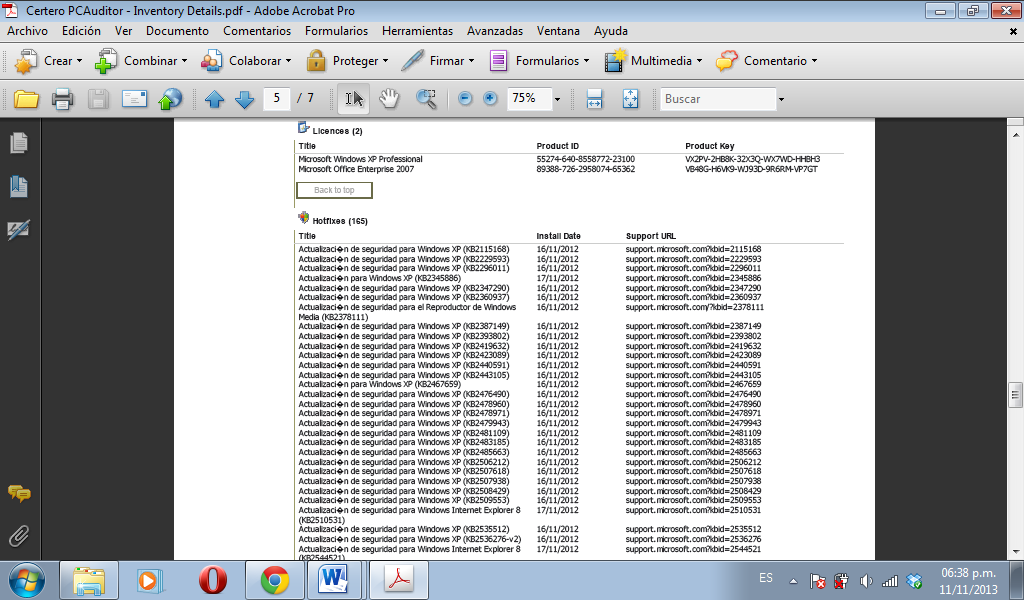


**SOFTWARE**

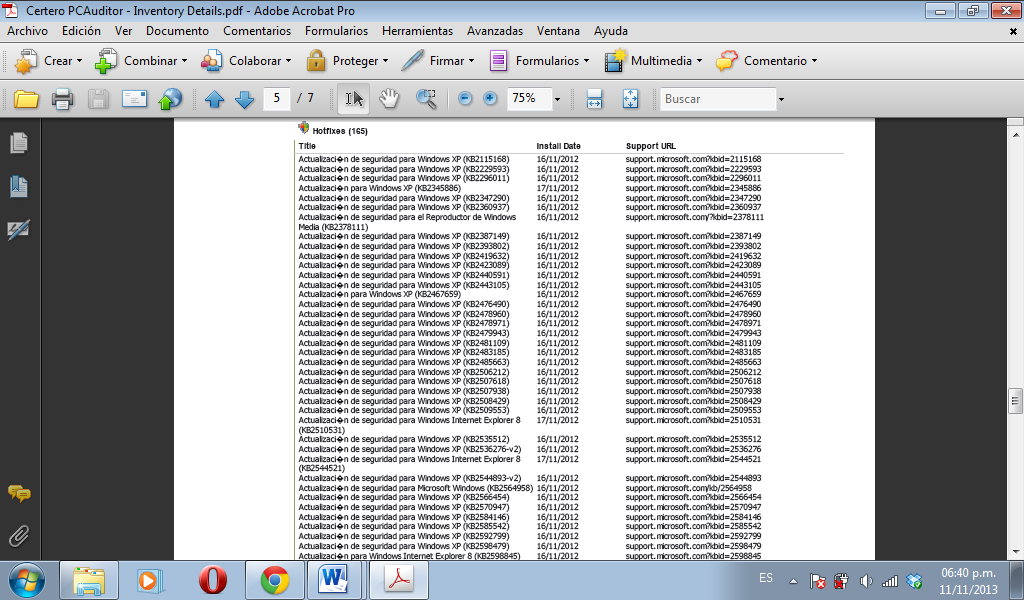
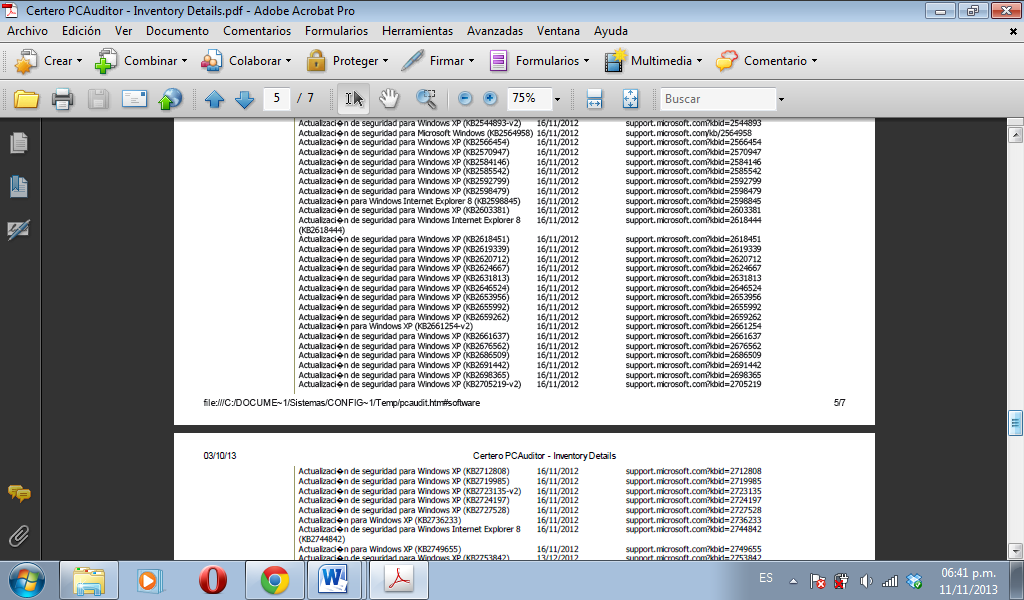


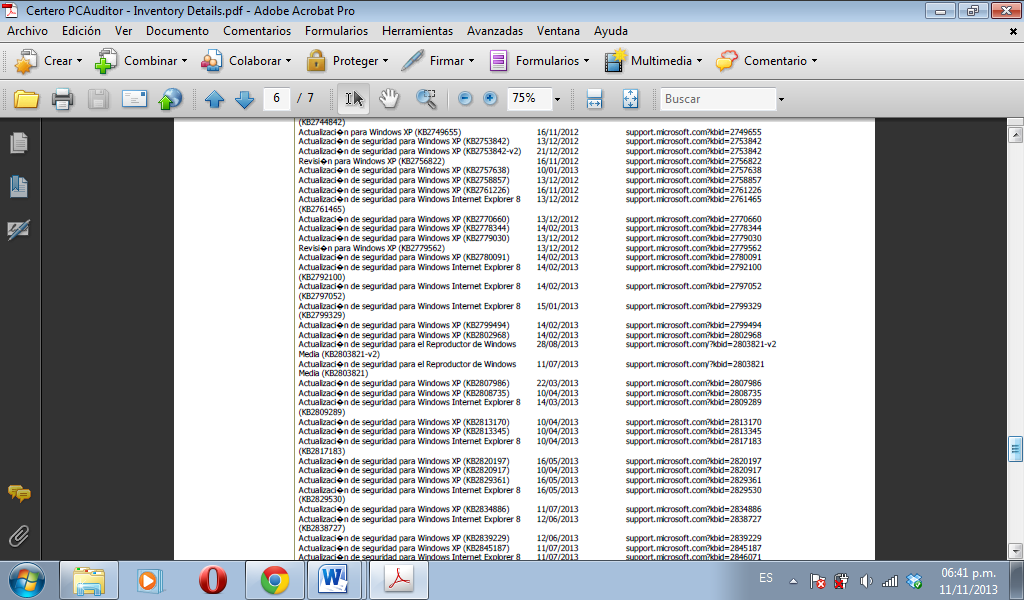


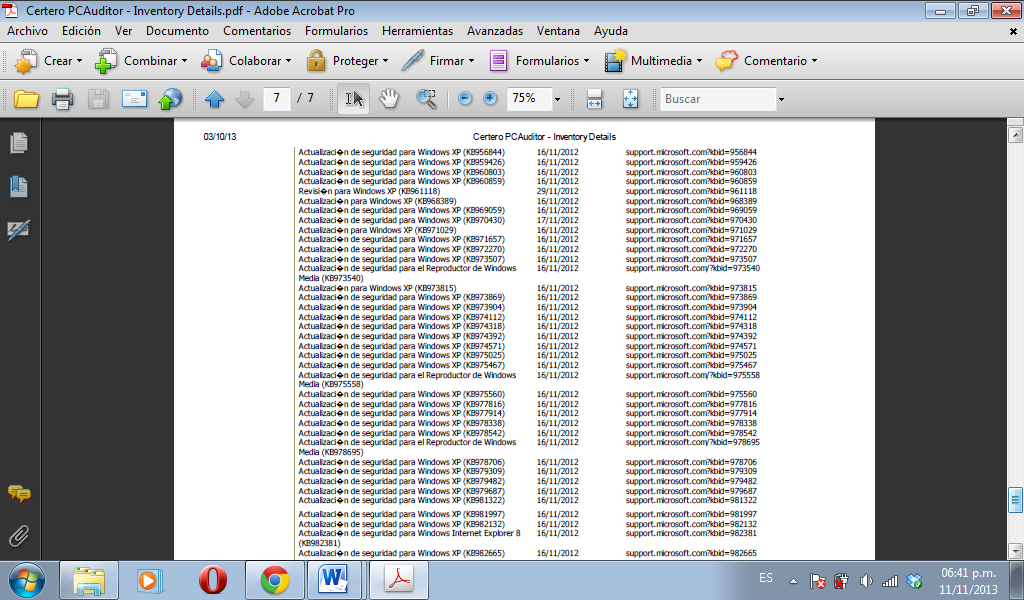
**LICENCIAS**



**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.

**El alcance de la auditoria nos mostrara si:**

* ¿Las condiciones de las salas de informática están acorde a las normas de
* seguridad industrial establecidas?
* ¿Los equipos de cómputo se encuentran en las condiciones mínimas requeridas
* para la prestación del servicio?
* ¿Las redes alámbricas e inalámbricas se encuentran protegidas con contraseña,
* para evitar la intromisión de personal ajeno a la institución?
* ¿La ofimática de la sala se encuentra debidamente legalizada?
* ¿Las personas a cargo del mantenimiento de las salas, son idóneas y están
* capacitadas para dar respuesta oportuna a las necesidades de la misma?
* ¿Actualmente se encuentra con una diagramación de red a prueba de fallos?

A continuación expondremos la realidad de cada una de los puntos que se auditaron en las instalaciones de El Independiente de Hidalgo así:

**2.1. Equipos de Cómputo:**

Se cuenta con una de salas de informática, la cuál será auditada de acuerdo a las normas que estén establecidas, se observará, y revisará de forma directa e indirecta los equipos, su instalación, ubicación y funcionamiento de las mismas.

Las cuales están bajo la responsabilidad de Lic. Susana López Galván Jefe de área de sistemas en redacción.

2.1.1 Cuantos equipos existen

|  |  |
| --- | --- |
| **No de Monitores** | **No de CPU`s** |
| 20 | 20 |

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

**Monitor:** Monitor de 14 pulgadas marca Dell

**Mouse:** Mouse alámbrico

**Teclado:** Teclado Acteck alámbrico

**Ups:** UPS Liebert Gxt6000t- 240xa.

**Reguladores de Voltaje:** Complet 1300va 8 contactos

# 3. PUNTOS DEBILES Y AMENAZAS.

**MATRIZ FODA(PROPUESTA)**

|  |  |
| --- | --- |
| FACTORES INTERNOS  Controlables | FACTORES EXTERNOS  No Controlables |
| **FORTALEZAS**  **(+)**  Personal competente.  Personal extraído de la Universidad.  Personal comprometido.  Equipo de cómputo acorde.  Buenas instalaciones. | **OPORTUNIDADES**  **(+)**  Nuevo crecimiento en el mercado  Expansión  Difusión y apoyo por parte de la Universidad |
| **DEBILIDADES**  de los equipos de computo   * Estaciones de trabajo fuera de servicio. * Mala ubicación del Site. * Débil ancho de banda * No se realiza mantenimiento a las estaciones de trabajo periódicamente. * Falta de no-breaks.   (-) | **AMENAZAS**   * Poca ventilación, lo que puede producir recalentamiento de los equipos. * El controlador de los dispositivos de teclado, mouse y red, puede fallar dejando incompleto el trabajo. * Falta de capacidad del UPS para todo el centro, ya que es muy corto el tiempo que tiene.   (-) |

**3.1. RECOMENDACIONES DE LA AUDITORIA**

Después de analizar las diferentes amenazas que se presentan con los equipos de cómputo, los auditores hemos encontrado las siguientes recomendaciones:

* Adquirir un ventilador para mantener en óptimas condiciones la ventilación de los equipos, pues con la que cuentan actualmente, no se considera prudente.
* Elaborar un plan de contingencia ya que en el momento que una unidad conectora de dispositivos falle.
* Dar una mejor ubicación al site.

**4. CONEXIONES ELÉCTRICAS**

Después de recorrer las salas de cómputo, hemos podido detallar que existe una correcta instalación eléctrica para los diferentes equipos y dispositivos que se manejan en las salas de sistemas.

La tendencia para este punto, es la certificación del cableado eléctrico del Independiente de Hidalgo.

# 4.1. PUNTOS DÉBILES Y AMENAZAS.

Las debilidades que podemos encontrar con el tipo de cableado son:

* No hay garantía de funcionamiento permanente de las maquinas en el momento de un corto.
* Las amenazas que encontramos son las siguientes:
* Posibilidad de corto circuito.
* En caso de daño, será difícil identificar qué cable fue, o en su defecto cambiarlo, será muy complicado.
* Daño en el software instalado en las maquinas por el apagado inesperado de la máquina, dado por el sobrecalentamiento causado por la falta de ventilación.
* Mayor control sobre el consumo de alimentos frente al equipo de cómputo.

# 4.2. RECOMENDACIONES

Con base en la norma y en un plazo no muy largo, dar solucionar de fondo que garanticen la correcta colocación del site.

# 5. CABLEADO ESTRUCTURADO.

El cableado si cumple con las normas, dado que se encuentra entubado dentro de tubos de plástico, evitando que los cables anden dispersos en el suelo.

## NORMA TIA/EIA-568-B

## Objetivos

TIA/EIA-568-B intenta definir estándares que permitirán el diseño e implementación de sistemas de cableado estructurado para edificios comerciales y entre edificios en entornos de campus. El sustrato de los estándares define los tipos de cables, distancias, conectores, arquitecturas, terminaciones de cables y características de rendimiento, requisitos de instalación de cable y métodos de pruebas de los cables instalados. El estándar principal, el TIA/EIA-568-B.1 define los requisitos generales, mientras que TIA/EIA-568-B.2 se centra en componentes de sistemas de cable de pares balanceados y el -568-B.3 aborda componentes de sistemas de cable de fibra óptica.

# 5.1. PUNTOS DÉBILES Y AMENAZAS.

Se hallan las siguientes amenazas:

* Es una mala imagen para la entidad no aplicar las normas.
* No existe garantía en el buen funcionamiento del cableado.

Las amenazas se pueden resumir en:

* Perdida de datos.
* Deficiencia en la comunicación entre equipos a nivel de red.

# 5.2. RECOMENDACIONES

Como auditores y basados en la norma mencionada en este documento, se le deja como recomendación, el estudio y la puesta en marcha de la instalación del cableado estructurado.

Lo anterior con el fin de evitar gastos en pequeñas reparaciones, que con el tiempo van a significar un gran costo.

# 6. CONEXIONES DE REDES

Por las conexiones que presenta se puede determinar que el tipo de red está basado en una de área local.

Porque llegamos a esta conclusión:

* Existen dos switch cuyo fin es interconectar conmutada las máquinas.
* Las máquinas están interconectadas a un único medio de comunicación.

# 6.1. PUNTOS DÉBILES Y AMENAZAS

* No se encuentran debilidades a causa de la red, ya que esta bien definida la topología que se esta utilizando para la distribución de información. La topología utilizada es la estrella, para que sea la principal la que pueda otorgar todos los permisos.

# 7. LICENCIAMIENTO DEL SOFTWARE

* Este es un punto bastante crítico, para cualquier entidad en el país, ya que por ley las entidades o empresas legalmente constituidas en el país, no pueden contar con software ilegal o mal conocido como pirata en sus diferentes estaciones de trabajo.
* Lo anterior de acuerdo a que el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 que obliga a las empresas a declarar si los problemas de software son o no legales.
* Basados en lo anterior y consientes que la universidad no cuenta con el total de licencias para la legalidad de su software, se tiene como tendencia que en un corto Plazo este impase este resuelto.

# 7.2. PLANES DE CONTINGENCIA.

En los papeles de trabajo de la auditoria pudimos observar que no existe ningún tipo de plan o procedimiento, en el cual se de una contingencia a posibles daños en la estaciones de trabajo o en su información.

Se recomienda:

Crear un plan de respaldo externo al que se tiene, ya que esta dentro de la misma empresa y en caso de pérdida total, se perdería toda la información.

Crear un plan alterno en caso de que se dañe algún equipo de cómputo, y más si se trata del principal que es el que distribuye toda la información al resto de los equipos.

# 7.2.1. PUNTOS DÉBILES Y AMENAZAS.

En este caso la debilidad está dada en no tener un modo de respaldar la información de carácter importante que hay en las estaciones de trabajo.

De igual forma es preocupante, no contar con unidades de cómputo que puedan reemplazar aquellas que por cualquier motivo queden fuera de servicio.

En lo que concierne a las amenazas podríamos destacar:

􀁸 No existe la forma de reemplazar las estaciones de trabajo en caso de daño.

􀁸 No hay un respaldo o un servidor donde se pueda almacenar la información de mayor importancia.

􀁸 En caso de daño de la red, no se cuenta con un proveedor certificado para una pronta solución.

Se debe tener en cuenta que la finalidad de este plan de contingencia es mantener el funcionamiento de la corporación universitaria, sin que esta sufra traumatismo alguno tecnológicamente.

# 7.3. NORMAS PARA USO DE LAS SALAS DE SISTEMAS

Después de realizar un recorrido por las diferentes salas de sistemas del periódico El Independiente de Hidalgo, se pudo observar que el personal consume alimentos, sin control alguno.

También se puede ver que los usuarios no están capacitados para el uso de herramientas de emergencia como extintor.

**Capítulo Primero**  
Definiciones para propósitos del presente reglamento

**Equipo computacional de trabajo**Se considera como equipo computacional de trabajo 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 administradas por la Dirección de Informática, además de los equipos instalados en las salas de cómputo centrales.

**Equipo computacional administrativo**Es todo aquel equipo adquirido por el Independiente de Hidalgo destinado a servir como apoyo a labores administrativas.

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

* Los reporteros del periódico El Independiente de Hidalgo.

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

* Los empleados, profesionistas de apoyo y directivos que tengan acceso a estos provilegios.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Segundo**  
Del uso de los equipos

El equipo computacional deberá utilizarse como herramienta de apoyo para labores de trabajo de los usuarios, ya sea en las salas destinadas como recinto de este equipo, como a través de servicios de comunicación remota.

El uso del equipo computacional es exclusivo para los usuarios del periódico. Cualquier persona que no esté considerada como tal y que desee hacer uso del equipo computacional deberá solicitar un permiso especial en la Dirección de Servicios Computacionales de la Dirección de Informática.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Tercero**Del acceso a las áreas de servicio computacional.

Del acceso a los servicios en equipos de cómputo centrales y servicios de red con autenticación

A todos los usuarios se les proporcionará identificador único de acceso (password) que podrá ser cambiada a voluntad por el usuario. Esto quiere decir, que las cuentas son personales e intransferibles.

El periódico El Independiente de Hidalgo se reserva el derecho de suspender el servicio a un usuario cuando se sospeche de un abuso o uso indebido del servicio.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Cuarto**Del comportamiento a observar

El comportamiento de todos los usuarios deberá ir de acuerdo a la moral y buenas costumbres.

Todo usuario deberá dar uso adecuado al equipo de cómputo, en el caso de que algún equipo resulte dañado por alguna acción atribuible al usuario, éste será acreedor a una sanción.

Cuando un usuario esté utilizando los servicios de comunicación electrónica, deberá observar las reglas que cada uno de estos servicios tenga dentro y fuera de la empresa. En el caso de las redes internacionales el usuario será responsable de conocer y seguir las reglas que tenga la comunicación por este medio.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Quinto**De la separación de equipos o equipos con acceso restringido

Sólo se podrá restringir el acceso a un equipo si éste tiene facilidades de ser administrado en forma automática por medio de la asignación de claves.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Sexto**De las prohibiciones

Las actividades que se contemplan en este reglamento incluyen, pero no se limitan, a las siguientes restricciones; quedando prohibido a todos los usuarios:

* Introducir alimentos, bebidas o fumar en las áreas de servicio.
* Utilizar grabadoras, radios o equipos de sonido sin audífonos en las áreas de servicio.
* Utilizar los equipos computacionales académicos como máquinas de juegos; esto incluye utilizar software de juegos o acceder a servicios que impliquen el uso de juegos interactivos. De esta restricción se exceptúa el software de simulación autorizado para su uso por el Departamento de Servicios Computacionales bajo solicitud del profesor encargado de la materia en que se requiera.
* Utilizar el equipo computacional para desarrollar programas o proyectos ajenos.
* Extraer equipo computacional académico o sus partes de las áreas de servicio.
* Alterar o dañar las etiquetas de identificación de cualquier equipo computacional académico.
* Extraer materiales de consumo del equipo computacional académico o de las salas.
* Dejar material para utilizarse el siguiente día en las áreas de servicio o aulas activas.
* Copiar software cuya licencia de uso lo prohiba.
* Alterar software instalado en el equipo computacional.
* Utilizar el equipo computacional o la infraestructura de comunicación asociada a él para acceder equipos locales o remotos a los que el usuario no tenga autorización explícita, o en su uso, intentar violar la seguridad de acceso de cualquier equipo computacional.
* Utilizar claves de acceso o cuentas de otros usuarios o permitir a otros usuarios utilizar la propia.
* Interrumpir las labores de otros usuarios mediante mensajes, cuando éstos expresen su inconformidad.
* Utilizar una identidad diferente a la propia (de otro usuario o ficticia) o actuar en forma anónima para enviar mensajes en forma electrónica.
* Llevar a cabo acciones que interfieran o puedan interferir con la operación normal de los equipos computacionales o de comunicación electrónica del Campus o de cualquier instalación accesible desde el mismo.
* Utilizar los medios de comunicación electrónica de forma que puedan atentar contra otros individuos o interferir en sus actividades.
* 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 el equipo para actividades o aplicaciones diferentes a aquellas para las cuales el equipo está destinado (Equipos de uso especial).
* Utilizar los equipos instalados en las salas para desplegar material obsceno o que atente contra los valores que promueve el Instituto.
* Utilizar las áreas operativas del sistema para el almacenamiento de archivos personales.
* Intentar quebrantar las medidas de seguridad del 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.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Séptimo**De las sanciones

Toda violación a este reglamento será sancionada de acuerdo al Reglamento General en el caso de los usuarios o por las autoridades correspondientes de la Institución en el caso del resto de los usuarios.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Octavo**De la 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 en los equipos de la Institución 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.

Todo usuario del cual se requiera consultar su información tendrá el derecho de estar presente en el momento de la consulta de la misma, que sólo podrá ser llevada a cabo, con la autorización respectiva y por escrito, por personal de la Dirección de Informática y de Auditoría Interna en conjunto.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Noveno**Observaciones Generales

La Dirección de Informática se reserva el derecho de utilizar los medios a su alcance para investigar posibles violaciones a este reglamento, siempre que sea respetada la confidencialidad de la información.

La Dirección de Informática se reserva el derecho de suspender o eliminar el acceso a cualquier equipo computacional a cualquier usuario, sin previo aviso al mismo, si el hacerlo es necesario para mantener la disponibilidad, seguridad e integridad de las operaciones para los demás usuarios de los recursos, o cuando se presuma alguna falta o violación a este reglamento u otros pertinentes que amerite este tipo de acciones para el proceso de investigación.

[Vuelve a inicio](http://publidinf.mty.itesm.mx/publidinfvirtual/reglamento/reglamento.htm#Inicio)

**Capítulo Décimo**  
De la observancia y vigilancia del presente reglamento

Dada la naturaleza del presente reglamento, su conocimiento y observancia son obligatorios para todos los usuarios académicos del equipo computacional. Su desconocimiento nunca podrá ser invocado como excusa para evitar las sanciones correspondientes.

El presente reglamento entrará en vigor a partir de la fecha de su publicación.

**7.3.1. PUNTOS DÉBILES Y AMENAZAS**

Son muchas las debilidades con las que cuentan las salas de cómputo caso de estudio entre ellas están:

* Falta de seguridad con el hardware.
* Consumo de alimentos.

Dentro de las amenazas se pueden encontrar:

* Daños a la infraestructura tecnológica.
* Daño de los elementos de hardware.

# Planeación de la auditoría

# CONTROLES

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.

b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles(principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.

c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.

d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

***CONTROL DE LOS DATOS FUENTE Y MANEJO CIFRAS DE CONTROL***

La mayoría de los Delitos por computadora son cometidos por modificaciones de datos fuente al:

1. Suprimir u omitir datos.
2. Adicionar Datos.
3. Alterar datos.
4. Duplicar procesos.

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

El primer nivel es el que puede hacer únicamente consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que solo puede hacer todos lo anterior y además puede realizar bajas.

NOTA: Debido a que se denomina de diferentes formas la actividad de transcribir la información del dato fuente a la computadora, en el presente trabajo se le denominará captura o captación considerándola como sinónimo de digitalizar (capturista, digitalizadora).

Lo primero que se debe evaluar es la entrada de la información y que se tengan las cifras de control necesarias para determinar la veracidad de la información, para lo cual se puede utilizar el siguiente cuestionario:

1. Indique el porcentaje de datos que se reciben en el área de captación

2. Indique el contenido de la orden de trabajo que se recibe en el área de captación de datos:   
Número de folio ( X) Número(s) de formato(s) (X )   
Fecha y hora de Nombre, Depto. ( X)   
Recepción ( ) Usuario ( )   
Nombre del documento (X ) Nombre responsable (X )   
Volumen aproximado Clave de cargo   
de registro ( ) (Número de cuenta) ( )   
Número de registros ( ) Fecha y hora de entrega de   
Clave del capturista ( ) documentos y registros captados ( X)   
Fecha estimada de entrega ( )

3. Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de datos:   
Firmas de autorización (X)   
Recepción de trabajos (X) Control de trabajos atrasados ( )   
Revisión del documento (X) Avance de trabajos (X)   
fuente (legibilidad, verificación de datos completos, etc.) (x)   
Prioridades de captación ( ) Errores por trabajo (x)   
Producción de trabajo (x) Corrección de errores (x)

Producción de cada operador ( ) Entrega de trabajos (x)   
Verificación de cifras Costo Mensual por trabajo ( )   
de control de entrada con   
las de salida. ( )

4. ¿Existe un programa de trabajo de captación de datos?   
a) ¿Se elabora ese programa para cada turno?   
Diariamente (x)   
Semanalmente ( )   
Mensualmente ( )   
b) La elaboración del programa de trabajos se hace:   
Internamente (x)   
Se les señalan a los usuarios las prioridades (x)

c) ¿Que acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?

Se está presionando al trabajador, dándole una llamada de atención, si éste reincide, se le hace una multa sobre su salario por reincidir.

5. ¿Quién controla las entradas de documentos fuente?

La encargada del área de sistemas.

6. ¿En qué forma las controla?

Según vaya recibiendo los documentos, los va guardando en la carpeta que le corresponde a cada usuario para que pueda estar disponible y de forma entendible para ella y los encargados de sistemas.

7. ¿Qué cifras de control se obtienen?

Sistema Cifras que se Observaciones   
Obtienen

8. ¿Qué documento de entrada se tienen?   
Sistemas Documentos Depto. que periodicidad Observaciones   
proporciona el documento

No se cuenta como tal con un documento de entrada de la información, todo se va haciendo de manera digital, lo único podría ser que cada edición final del periódico impresa, se van almacenando en un folder y se llaman banderas, y se clasifican por mes y por año.

9. ¿Se anota que persona recibe la información y su volumen?   
SI ~~NO~~

10. ¿Se anota a que capturista se entrega la información, el volumen y la hora?   
SI ~~NO~~

11. ¿Se verifica la cantidad de la información recibida para su captura?   
~~SI~~ NOPero no se hace al momento, se hace un día después.

12. ¿Se revisan las cifras de control antes de enviarlas a captura?   
SI ~~NO~~

13. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?   
SI ~~NO~~

14. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?

No, escrito no está estipulado, simplemente las impresiones que salieron con errores, se reciclan para cuidar el medio ambiente.

15. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?

NO

16. Si se queda en el departamento de sistemas, ¿Por cuánto tiempo se guarda?

Por el momento se tiene planeado que se guarde por 3 años, pero dado que la empresa apenas cuenta con 4 años de existencia, se quedarían con muy poca información almacenada, entonces por eso se esperarán un poco más de tiempo.

17. ¿Existe un registro de anomalías en la información debido a mala codificación? NO

18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?

No

19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?

Si

20. ¿Se hace una relación de cuándo y a quién fueron distribuidos los listados? No, aunque como tal ya saben a qué persona le toca, sólo les hace falta tenerlo de forma escrita.

21. ¿Se controlan separadamente los documentos confidenciales?   
Si

22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?   
Si

23. ¿Existe un registro de los documentos que entran a capturar?   
No

24. ¿Se hace un reporte diario, semanal o mensual de captura?   
Diario

25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?

No

26. ¿Se lleva un control de la producción por persona?

No de forma escrita.

27. ¿Quién revisa este control?

Lo realiza la encargada del área de sistemas

28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

No

# CONTROL DE OPERACIÓN

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

El objetivo del presente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de cómputo?   
SI ( ) NO (X )

2. ¿Están actualizados los procedimientos?   
SI ( ) NO (X )

3. Indique la periodicidad de la actualización de los procedimientos:

Semestral ( )   
Anual ( )   
Cada vez que haya cambio de equipo (X )

4. Indique el contenido de los instructivos de operación para cada aplicación: (propuesta)

Identificación del sistema ( )   
Identificación del programa ( )   
Periodicidad y duración de la corrida ( )   
Especificación de formas especiales (X )   
Especificación de cintas de impresoras ( )   
Etiquetas de archivos de salida, nombre, (X )   
archivo lógico, y fechas de creación y expiración   
Instructivo sobre materiales de entrada y salida (X )   
Altos programados y la acciones requeridas ( )   
Instructivos específicos   
a los operadores en caso de falla del equipo ( )   
Instructivos de reinicio ( )   
Procedimientos de recuperación para proceso de   
gran duración o criterios ( )   
Identificación de todos los   
dispositivos de la máquina a ser usados ( )   
Especificaciones de resultados   
(cifras de control, registros de salida por archivo, etc. ) ( )

5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?   
SI ( ) NO (X )

6. ¿Son suficientemente claras para los operadores estas órdenes?   
SI ( ) NO ( X)

7. ¿Existe una estandarización de las ordenes de proceso?   
SI ( ) NO ( X)

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados. propuesta  
SI ( ) NO ( X)

9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?   
Primero que entra, primero que sale (X )   
se respetan las prioridades, ( )   
Otra (especifique) ( )

10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?   
SI (X ) NO ( )

11. ¿Quién revisa este reporte en su caso?

Primero pasa por la encargada de sistemas y si la situación no está al alcance de sus manos, pasa por el jefe de redacción, hasta la directora.

12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.

Dado que la función que utilizan en cada equipo es básica, puesto que utilizan la paquetería de office, y de ahí sólo Word, el uso de las computadoras no exige un uso rudo. Caso contrario con los paginadores, quienes ocupan equipos MAC, pero el cual es el apropiado para poder realizar sus actividades de forma adecuada.

13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?

NO

14. ¿Cómo se actúa en caso de errores?

Se le llama a la encargada de sistemas y es la encargada de darle solución al mismo.

15. ¿Existen instrucciones específicas para cada proceso, con las indicaciones pertinentes? No

16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

No

17. ¿Puede el operador modificar los datos de entrada?

No, todo está bien definido en cuanto a los permisos, los únicos que tienen que modificar a los reporteros, son los correctores y son los únicos que pueden ver y editar la información.

18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo? No

19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas? Si

20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran? No

21. ¿Las intervenciones de los operadores:

Son muy numerosas? SI ( ) NO (x )   
Se limitan los mensajes esenciales? SI ( ) NO (x )   
Otras (especifique)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?   
SI ( ) NO (x )   
23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?

Se les piden las famosas guías, para saber qué es lo que realizará cada quien, la forma en la que se dividirán el trabajo.

24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?   
SI ( ) NO (x )

25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?   
Si ( )   
por máquina ( x)   
escrita manualmente ( )   
NO ( )   
26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.

No

27.¿Existen procedimientos para evitar las corridas de programas no autorizados?   
SI (x ) NO ( )

28. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.

No está definido como tal, entre ellos mismos se ponen de acuerdo si algún día por alguna causa se tiene que faltar o hay algún cambio

29. Verificar que sea razonable el plan para coordinar el cambio de turno.

Si

30. ¿Se hacen inspecciones periódicas de muestreo?   
SI ( ) NO (x )

31. Enuncie los procedimientos mencionados en el inciso anterior:

32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?   
SI ( ) NO ( x)

33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?   
SI (X ) NO ( )   
¿Cómo? La encargada del área de sistemas, es la que regula los permisos, para que los usuarios tengan o no la capacidad para poder acceder a la información que según deseen.

34. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.

Si están restringidos

35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?   
SI ( ) NO (x )

36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?   
SI ( ) NO (x )

37. ¿Durante cuánto tiempo? indefinido

38. ¿Qué precauciones se toman durante el periodo de implantación?

Que no se pierda la información, ni los permisos.

39. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación? El encargado de sistemas del área administrativa

40. ¿Se catalogan los programas liberados para producción rutinaria?   
SI ( ) NO ( x)

41. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.

Ninguno

42. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.

Se tienen almacenados en el servidor, pero cuando llegan a su máxima capacidad, se encarga el personal de sistemas de almacenarlo en cajas dentro de una bodega para cualquier imprevisto que se pueda sucitar.

43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?   
SI (x ) NO ( )

44. Indique como está organizado este archivo de bitácora.

1. Por fecha (x )
2. por fecha y hora ( )
3. por turno de operación ( )
4. Otros ( )

45. ¿Cuál es la utilización sistemática de las bitácoras?

Para saber quién ingreso y le dio uso a ese archivo

46. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?

Redacción, paginación, corrección.

47. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.

No hay

48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?   
SI (x ) NO ( )

49. ¿Cómo se controlan los procesos en línea?

Mediante el tráfico de la red.

50. ¿Se tienen seguros sobre todos los equipos?   
SI ( ) NO ( x)

51. ¿Conque compañía?   
Solicitar pólizas de seguros y verificar tipo de seguro y montos.

52. ¿Cómo se controlan las llaves de acceso (Password)?.   
La encargada de sistemas al crearles su usuario, les pide que ellos mismo coloquen su contraseña, para así evitar cualquier problema de pérdida de información.

# CONTROLES DE SALIDA

1. ¿Se tienen copias de los archivos en otros locales?

No

2. ¿Dónde se encuentran esos locales? No hay

3. ¿Qué seguridad física se tiene en esos locales?

No hay

4. ¿Qué confidencialidad se tiene en esos locales?

No hay

5. ¿Quién entrega los documentos de salida?

La encargada de sistemas se los pasa al área administrativa, quienes se encargan de almacenarlos.

6. ¿En qué forma se entregan?

Las banderas se entregan en forma física.

7. ¿Qué documentos?

El documento del periódico día.

8. ¿Qué controles se tienen?

Dichas impresiones del periódico final, se almacenan en banderas, para guardarse por mes y al final por año.

9. ¿Se tiene un responsable (usuario) de la información de cada sistema? ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

De dicha información se encarga la encargada de derechos humanos.

10. ¿Se destruye la información utilizada, o bien que se hace con ella?

Destruye ( ) Vende ( ) Tira ( ) Otro recicla

# CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no sólo en la unidad de informática, sino en la dependencia de la cual se presta servicio. Una dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de estos archivos, de modo que servirán de base a registros sistemáticos de la utilización de estos archivos, de modo que sirvan de base a los programas de limpieza (borrado de información), principalmente en el caso de las cintas.

Además se deben tener perfectamente identificados los carretes para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando además los tiempos de procesos.

# CONTROL DE ALMACENAMIENTO MASIVO

OBJETIVOS

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados al site tienen:

1. Aire acondicionado ( x)
2. Protección contra el fuego ( )
3. (señalar que tipo de protección )\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Cerradura especial (x )
5. Otra

2. ¿Tienen en el site protección automática contra el fuego?   
SI ( ) NO ( x)   
(señalar de que tipo) un extintor

3. ¿Qué información mínima contiene el inventario del site?

Número de serie o carrete (x )   
Número o clave del usuario ( )   
Número del archivo lógico ( )   
Nombre del sistema que lo genera ( )   
Fecha de expiración del archivo ( )   
Fecha de expiración del archivo ( )   
Número de volumen ( )   
Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?   
SI ( ) NO (x )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?   
SI ( ) NO (x )

6. ¿Qué tan frecuentes son estas discrepancias?   
Hasta que se satura de información.

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?   
SI ( ) NO (x )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?   
SI (x ) NO ( )   
¿Cómo? Aunque sólo el personal autorizado lo sabe

9. ¿Existe un control estricto de las copias de estos archivos?   
SI ( ) NO (x )

10. ¿Qué medio se utiliza para almacenarlos?   
Mueble con cerradura ( )   
Bóveda ( )   
Otro(especifique)\_Servidor tipo mirror .

11. Este almacén esta situado:   
En el mismo edificio del departamento (x )   
En otro lugar ( )   
¿Cual?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?   
SI ( x) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?   
SI ( ) NO (x )   
14. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?   
SI ( x) NO ( )

15 ¿Se tiene un responsable, por turno, de la cintoteca y discoteca?   
SI (x ) NO ( )

16. ¿Se realizan auditorías periódicas a los medios de almacenamiento?   
SI (x ) NO ( )

17. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento? No se tienen

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?   
SI (x ) NO ( )

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?   
SI ( ) NO (x )

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?   
SI ( ) NO (x )

21. ¿Se lleva control sobre los archivos prestados por la instalación?   
SI ( ) NO ( x)

22. En caso de préstamo ¿Conque información se documentan?   
Nombre de la institución a quién se hace el préstamo.

1. fecha de recepción ( )
2. fecha en que se debe devolver ( )
3. archivos que contiene ( )
4. formatos ( )
5. cifras de control ( )
6. código de grabación ( )
7. nombre del responsable que los presto ( )
8. otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

Ninguno

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?   
SI (x ) NO ( )

25. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?   
SI ( x) NO ( )

26. ¿La operación de reemplazo es controlada por el cintotecario?   
SI (x ) NO ( )

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?   
SI (x ) NO ( )

28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?   
SI ( ) NO (x )

29. ¿Estos procedimientos los conocen los operadores?   
SI ( ) NO ( x)

30. ¿Con que periodicidad se revisan estos procedimientos?   
MENSUAL ( ) ANUAL ( )   
SEMESTRAL ( ) OTRA ( )

31. ¿Existe un responsable en caso de falla?   
SI ( x) NO ( )

32. ¿Explique qué políticas se siguen para la obtención de archivos de respaldo? Se guarda la información en un servidor de tipo mirror.

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?   
SI ( ) NO (x )

34. ¿Lo conoce y lo sigue el cintotecario?   
SI ( ) NO ( x)

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?   
SI ( ) NO ( x)

¿Con qué frecuencia?

# CONTROL DE MANTENIMIENTO

Como se sabe existen básicamente tres tipos de contrato de mantenimiento: El contrato de mantenimiento total que incluye el mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no incluye partes. El contrato que incluye refacciones es propiamente como un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno. Este tipo de contrato es normalmente mas caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento es “por llamada”, en el cual en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para componerlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina a donde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como “en banco”, y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y este hace una cotización de acuerdo con el tiempo necesario para su compostura más las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe primero analizar cual de los tres tipos es el que más nos conviene y en segundo lugar pedir los contratos y revisar con detalles que las cláusulas estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigirle el cumplimiento del contrato de debe tener un estricto control sobre las fallas, frecuencia, y el tiempo de reparación.

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato). No se tiene

2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?   
SI ( ) NO ( X)

3. ¿Se lleva a cabo tal programa?   
SI ( ) NO ( X)

4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?   
SI ( ) NO (X )

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido? Se reemplaza de forma temporánea   
SI ( ) NO ( X)

6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.-   
SI ( ) NO ( x)   
¿Cual?

8. ¿Cómo se notifican las fallas?

En caso de falla en el equipo, se le avisa a la encargada de sistemas, quien da paso a dar soluciones.

9. ¿Cómo se les da seguimiento?

Se le pregunta si todo bien.

# ORDEN EN EL CENTRO DE CÓMPUTO

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:

Semanalmente ( ) Quincenalmente ( )   
Mensualmente ( ) Bimestralmente ( )   
No hay programa ( ) Otra (especifique) (x ) Se realiza semestrealmente, con el cambio de chico de servicio social

2. Existe un lugar asignado a las cintas y discos magnéticos?   
SI (x ) NO ( )

3. ¿Se tiene asignado un lugar específico para papelería y utensilios de trabajo?   
SI (x ) NO ( )

4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca?   
SI ( ) NO (x )

5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?   
SI ( ) NO (x )

6. Indique la periodicidad con que se limpian las unidades de cinta:

Al cambio de turno ( ) cada semana ( )   
cada día ( ) otra (especificar) (x cada que llega a su máxima capacidad )

7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?   
SI ( ) NO ( x) (Sólo fumar está prohibido, dado que es un espacio cerrado)

8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?   
SI ( x) NO ( )

9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?   
SI (x ) NO ( )

10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo:

No se ha dado dicho caso

# 1.5.- MODELOS DE CONTROL

En la actualidad existen una gran cantidad de modelos de control interno.

Los modelos de control interno COSO y COBIT son los dos modelos más difundidos en la actualidad.

COSO está enfocado a toda la organización, contempla políticas, procedimientos y estructuras organizativas además de procesos para definir el modelo de control interno.

Mientras que COBIT (Control Objectives for Information and Related Technology, Objetivos de Control para Tecnología de Información y Tecnologías relacionadas) se centra en el entorno IT, contempla de forma específica la seguridad de la información como uno de sus objetivos, cosa que COSO no hace. Además el modelo de control interno que presenta COBIT es más completo, dentro de su ámbito.

Existen otros tipos de modelos los cuales se mencionan a continuación:

OECD (Organization for Economic Cooperation and Development)

GAPP (Generaly Accepted Principles and Practices). National Institute of Standards and Technology (NIST)

BS 7799 (British Standard Institute)

SAC (Security Auditability and Control). The Inst. of Internal Audit.

COSO (Internal Control Integrated Framework. Committee of Sponsoring Organizations)

SSE CMM (Systems Security Engineering Capability Maturity Model)

National Security Agency (NSA) Defense- Canada.

CoCo (Criteria of Control Board of The Canadian Instituteof Chartered Accountants.)

ITCG (Information Technology Control Guidelines). Canadian Institute of Chartered Accountants(CICA)

GASSP (Generaly Accepted System Security Principles). International

Information Security Foundation (IISF)

Cobit (Control Objectives for Information and Related Technologies) FISCAM (Federal Information Systems Controls Audit Manual).

GAO

SysTrust (AICPA/CICA SysTrust Principles and Criteria for System Reliability)

SSAG (System Self-Assessment Guide for Information Technology Systems). NIST

**COBIT – DEFINICIÓN**

Es un marco de control interno de TI.

Parte de la premisa de que la TI requiere proporcionar información para lograr los objetivos de la organización.

Promueve el enfoque y la propiedad de los procesos.

Apoya a la organización al proveer un marco que asegura que:

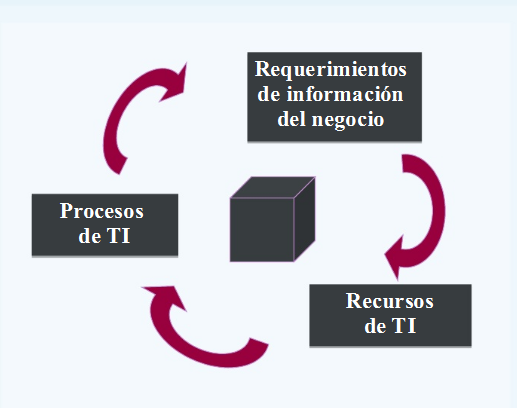
La Tecnología de Información (TI) esté alineada con la misión y visión.

LA TI capacite y maximice los beneficios.

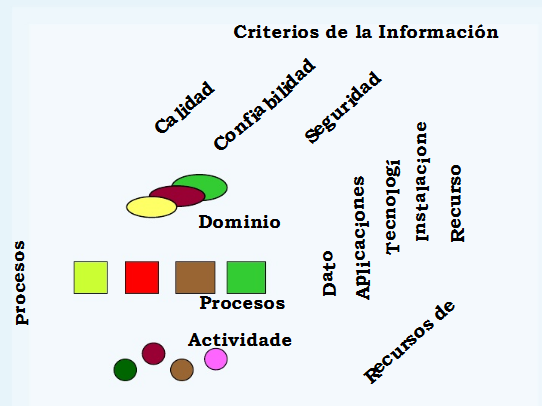
Los recursos de TI sean usados responsablemente.

Los riesgos de TI sean manejados apropiadamente.

**COBIT – PRINCIPIOS**

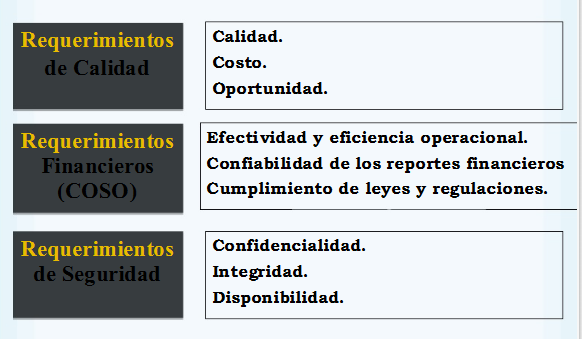


**COBIT – ESTRUCTURA**



COBIT – REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO

COBIT combina los principios contenidos por modelos existentes y conocidos, como COSO, SAC Y SAS.



COBIT – REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO

Efectividad: Información relevante y pertinente, proporcionada en forma oportuna, correcta, consistente y utilizable

Eficiencia: Empleo óptimo de los recursos.

Confidencialidad: Protección de la información sensitiva contra divulgación no autorizada

Integridad: Información exacta y completa, así como válida de acuerdo con las expectativas de la organización.

Disponibilidad: accesibilidad a la información y la salvaguarda de los recursos y sus capacidades.

Cumplimiento: Leyes, regulaciones y compromisos contractuales.

Confiabilidad: Apropiada para la toma de decisiones adecuadas y el cumplimiento normativo

COBIT – PROCESOS DE TI – TRES NIVELES



**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, en caso 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**  **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%

7 X

**X = 21.87**

􀂙 **Para hallar el NO**

32 100%

19 X

**X = 59.37**

**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 cómputo esta |  | *x* |  |  |  |
| Los accesos de salida son |  |  | *x* |  |  |

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria física.

**2. Identificación del Cliente**

Departamento De Sistemas, área de redacción

**3. Identificación de la Entidad Auditada**

Caso de estudio periódico El Independiente de Hidalgo.

**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.
* No existe un calendario de mantenimiento
* Falta de ventilación.
* Faltan salidas al exterior debido a la infraestructura del edificio.

**6. Alcance de la auditoria**

* Nuestra auditoria, comprende el presente periodo julio-diciembre de 2013 y se ha realizado especialmente al caso de estudio del periódico El Independiente de Hidalgo del área de sistemas y redacción 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:**

**8. Recomendaciones**

* Reubicación de los equipos de cómputo ubicados junto al site.
* Implantar equipos de ventilación
* Implantar salidas de emergencia.
* Elaborar un calendario de mantenimiento de rutina periódico.
* Capacitar al personal para uso de extintores.

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PLANEAMIENTO** | **EJECUCIÓN** | **INFORME** |
| **FECHAS** | **01 De Agosto al 30 Septiembre** | **01 DE OCTUBRE AL 01 DE NOVIEMBRE** | **13 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
| **Gómez Rueda Luis Alberto** | **Auditor Líder** |
| **Picazo Hernández Francisco Javier** | **Auditor junior** |
| **Hernández Montes Ignacio** | **Auditor junior** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**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%

10 X

**X = 41.66**

􀂙 **Para hallar el NO**

24 100%

13- X

**X = 54.16**

**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 del 2013 y se ha realizado especialmente al periódico El Independiente de Hidalgo 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 plan de respaldo.

􀁸 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** | **13 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
| **Gómez Rueda Luis Alberto** | **Auditor Líder** |
| **Picazo Hernández Francisco Javier** | **Auditor Junior** |
| **Hernández Montes Ignacio** | **Auditor Junior** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**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**  **x** |  |  |
| 16. ¿El acceso a la red Wi-fi tiene password? | **x** |  |  |

**Auditoria de Redes:**

􀂙 **Para hallar el SI**

16 100%

4- X

**X = 25**

􀂙 **Para hallar el NO**

16 100%

11- X

**X = 68.75**

**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 cómputo |  |  |  |  | *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* |  |  |  |  |

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 2013 y se ha realizado especialmente al área de Informática del periódico El Independiente de Hidalgo, 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** | **13 DE NOVIEMBRE** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| **APELLIDOS NOMBRES** | **CARGOS** |
| **Gómez Rueda Luis Alberto** | **Auditor Líder** |
| **Picazo Hernández Francisco Javier** | **Auditor Junior** |
| **Hernández Montes Ignacio** | **Auditor Junior** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**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.

Es muy importante contar con un equipo de auditoría interna para trabajar en los detalles desde el principio y mantener una mejor imagen de la empresa, además son cosas necesarias, que tienen que ser vistas como una inversión, que si se logra conocer los detalles de las faltas con anticipación, puede ser un coste muy benéfico para la institución el prevenir que el reparo.

**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 personas auditores certificados y con un auditor Líder**
* **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**

* El periódico El Independiente de Hidalgo no cuenta con documentación:
* 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 | DIRECTOR DEL DEPARTAMENTO DE INFORMATICA | 6 MESES | 1 AÑO |
| Plan de redes | DIRECTOR DEL DEPARTAMENTO DE INFORMATICA | 6 meses | 1 año |
| Plan de Ofirmática | DIRECTOR DEL DEPARTAMENTO DE INFORMATICA | 6 meses | 1 año |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* El personal entrevistado mostró 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 encuentra evidencia documental de que se realice la evaluación del desempeño de los procesos. Ejemplo: “Proyecto CITEQ, según la Bitácora del CEN”, “Laboratorio de Análisis de aguas de abastecimiento y residuales, según la bitácora del CEN”. * No se encuentra evidencia documental de que se realice la evaluación de la realización de los productos. Ejemplos: Proyecto de evaluación de poliquetas como degradadores de sedimentos contaminados.(DCI) |