AUDITORIA DE SISTEMAS

****

**AUDITORIA SALAS DE SISTEMAS**

**H CONSULTORES**

**AUDITORES**

**David Zahid Jiménez Grez.**

**Jonathan Salas Hernández.**

**Adalberto Vargas Moreno.**

**Christian Yamil Castillo Covarrubias.**

AUDITORIA

DE SISTEMAS

**INTRODUCCIÓN**

A principios del siglo XXI, los sistemas de información se convirtieron en las herramientas más poderosas para poder materializar uno de los conceptos más importantes y necesarios para cualquier empresa: los sistemas de información de la empresa.

Hoy en día, la informática está inmersa en la gestión integral de la empresa, es por eso que las normas y estándares informáticos deben de estar sometidos a los generales de la misma. Consecuentemente, las empresas informáticas forman parte de lo que se ha denominado el *management* o gestión de la empresa.

Es necesario aclarar que la informática no administra en sí la empresa, sin embargo sí ayuda a la toma de decisiones. La auditoría informática existe debido a la importancia de la informática en el funcionamiento de una empresa.

Con frecuencia, el término *auditoría* se emplea de una forma incorrecta, ya que se ha considerado como una evaluación cuyo propósito es señalar errores y fallas a diestra y siniestra. Debido a esto último, se ha adoptado la frase “tiene auditoría” como un sinónimo de que en tal empresa se realizó una auditoría y se habían detectado fallas anteriormente.

**CONCEPTO DE CALIDAD**

El término calidad es ambiguamente definido y pocas veces comprendido, esto se debe a que:

La calidad no es una sola idea, es un concepto multidimensional;

La dimensión de calidad incluye el interés de la entidad, el punto de vista de la entidad, y los atributos de la entidad;

Por cada concepto existen diferentes niveles de abstracción;

Varía para cada persona en particular.

Una definición que se podría dar de calidad sería:

*Conjunto de propiedades y de características de un producto o servicio, que*

*le confieren aptitud para satisfacer unas necesidades explícitas o implícitas.*

**Evolución Histórica**

* Inspección/detección de errores: hasta los años 40.
* Inicialmente el trabajo era artesanal y el control existente era individual, independiente de cada tarea.
* En el año 1918, Ford Motor Company, monta la Primera cadena de montaje y en 1930 Laboratorios Bel la pone en marcha.

**Control (estadístico) de calidad: hasta los años 80.**

El mercado es poco competitivo. Precio de venta es fijado por el fabricante en función de los costes.

La principal función es impedir que el producto defectuoso llegue al cliente. Se persigue conseguir uniformidad de servicio.

El concepto de control de calidad es igual a “problema a resolver”. Se utilizan técnicas estadísticas para controlar la calidad del departamento de producción.

Se destacan en este periodo: Japón y Calidad total (1940-70). Deming,

Ishikawa, Juran, Crosby,…

**Garantía de calidad: a partir de los 80.**

El mercado se caracteriza por ser competitivo y de oferta. El precio de venta es fijado por el mercado. Entran en juego la planificación y medida de la calidad. Se implantan modelos de calidad que afectan a todos los departamentos.

1980. Interés por la calidad en los EEUU. TQM

1987. Premio *Malcom Baldrige Quality Award*

*1987.* ISO 9000. A partir de las normas británicas

1992. Premio Europeo a la calidad de la EFQM.

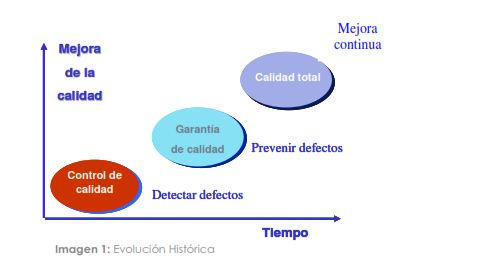
**Gestión de calidad hoy.**

Se busca un impacto estratégico y la oportunidad de ventaja competitiva.

Tienen relevancia conceptos como: Planificación, fijación de objetivos, coordinación, formación, adaptación de toda la organización.

La calidad afecta a la sociedad en general: directivos, trabajadores, clientes.

Se toma como “una filosofía, una cultura, una estrategia, un estilo de gerencia de la empresa”.



**Algunos conceptos**

Calidad: “Conjunto de propiedades y características de un producto o servicio que le confieren su aptitud para satisfacer unas necesidades explícitas o implícitas”

Control de calidad: “Conjunto de técnicas y actividades de carácter operativo, utilizadas para verificar los requerimientos relativos a la calidad del producto o servicio”.

Garantía de calidad: “Conjunto de acciones planificadas y sistemáticas necesarias para proporcionar la confianza adecuada de que un producto o servicio satisfará los requerimientos dados sobre calidad”.

Gestión de la calidad: “Aspecto de la función de gestión que determina y aplica la política de la calidad, los objetivos y las responsabilidades y que lo realiza con medios tales como la planificación de la calidad, el control de la calidad, la garantía de calidad y la mejora de la calidad”.

La gestión de la calidad es responsabilidad de todos los niveles ejecutivos, pero debe estar guiada por la alta dirección.

Su realización involucra a todos los miembros de la organización. En la gestión de la calidad, se tienen en cuenta también criterios de rentabilidad.

Sistema de gestión de la calidad: “Conjunto de la estructura de la organización, de responsabilidades, procedimientos, procesos y recursos que se establecen para llevar a término la gestión de calidad”. • Debe tener el volumen y alcance suficiente para conseguir los objetivos de calidad.

• Está fundamentalmente previsto para satisfacer las necesidades internas de la organización.).

• Para finalidades contractuales o vinculantes en la valoración de la calidad, se puede exigir que se ponga de manifiesto la realización de ciertos elementos del sistema de gestión de la calidad.

**Calidad del Software**

*“La calidad del software es el grado con el que un sistema, componente o proceso cumple los requerimientos especificados y las necesidades o expectativas del cliente o usuario”. (*IEEE, Std. 610-1990).

*“Concordancia del software producido con los requerimientos explícitamente establecidos, con los estándares de desarrollo prefijados y con los requerimientos implícitos no establecidos formalmente, que desea el usuario”* (Pressman, 1998).

Factores que determinan la calidad del software:

Se pueden clasificar en dos grandes grupos (Pressman):

Factores que pueden ser medidos directamente.

Factores que sólo pueden ser medidos indirectamente. Se centran en tres aspectos importantes de un producto software (McCall):

Características operativas: Corrección, fiabilidad, eficiencia, seguridad (Integridad) y facilidad de uso.

Capacidad de soportar los cambios: Facilidad de mantenimiento, flexibilidad y facilidad de prueba.

Adaptabilidad a nuevos entornos: Portabilidad, reusabilidad e interoperabilidad.

CONCEPTO DE SEGURIDAD

**Seguridad de la Información**

La seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada.

Los términos Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o la nueva línea de productos caigan en manos de un competidor o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma. Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Integridad: Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

Disponibilidad: La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

**Seguridad Informática**

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

***Objetivos de la seguridad informática:***

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres elementos que conforman los activos:

Información: Es el objeto de mayor valor para una organización. El objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

Equipos que la soportan: Software, hardware y organización.

Usuarios: Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

**INDICE DEL PROYECTO DE AUDITORIA DE SISTEMAS**

[CAPÍTULO I: INVESTIGACIÓN PRELIMINAR 2](#_Toc389023002)

[CONSIDERACIONES PREVIAS 2](#_Toc389023003)

[PLANEACIÓN DE LA AUDITORÍA 5](#_Toc389023004)

[Revisión Detallada 6](#_Toc389023005)

[Pruebas de Controles de los Usuarios 7](#_Toc389023006)

[Pruebas Sustantivas 7](#_Toc389023007)

[Examen y Evaluación de la Información 8](#_Toc389023008)

[EVALUACIÓN DEL ANÁLISIS 10](#_Toc389023009)

[EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA 12](#_Toc389023010)

[EVALUACIÓN DEL DESARROLLO DEL SISTEMA 14](#_Toc389023011)

[CONTROL DE PROYECTOS 15](#_Toc389023012)

[Control de diseño de sistemas y programación 18](#_Toc389023013)

[Forma de Implementación 20](#_Toc389023014)

[ENTREVISTA A USUARIOS 21](#_Toc389023015)

[Controles 24](#_Toc389023016)

[CONTROL DE OPERACIÓN 28](#_Toc389023017)

[Controles de Salida 33](#_Toc389023018)

[CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO 34](#_Toc389023019)

[ORDEN EN EL CENTRO DE CÓMPUTO 39](#_Toc389023020)

[MODELOS DE CONTROL 40](#_Toc389023021)

[ADMINISTRACIÓN 46](#_Toc389023022)

[A NIVEL DEL ÁREA DE INFORMÁTICA 46](#_Toc389023023)

[Objetivos a corto plazo: 46](#_Toc389023024)

[Objetivos a largo plazo. 46](#_Toc389023025)

[RECURSOS MATERIALES Y TECNICOS 46](#_Toc389023026)

[Estudios de viabilidad. 46](#_Toc389023027)

[Número de equipos, localización y las características 46](#_Toc389023028)

[Fechas de instalación de los equipos y planes de instalación. 46](#_Toc389023029)

[Contratos vigentes de compra, renta y servicio de mantenimiento. 46](#_Toc389023030)

[Contratos de seguros. 47](#_Toc389023031)

[Convenios que se tienen con otras instalaciones. 47](#_Toc389023032)

[Configuración de los equipos y capacidades actuales y máximas. 47](#_Toc389023033)

[Planes de expansión. 47](#_Toc389023034)

[Ubicación general de los equipos. 47](#_Toc389023035)

[Políticas de operación. 47](#_Toc389023036)

[Políticas de uso de los equipos. 47](#_Toc389023037)

[SISTEMAS 49](#_Toc389023038)

[Manual de procedimientos de los sistemas. 49](#_Toc389023039)

[Descripción genérica. 49](#_Toc389023040)

[Diagramas de entrada, archivos, salida. 50](#_Toc389023041)

[Fecha de instalación de los sistemas. 50](#_Toc389023042)

[Proyecto de instalación de nuevos sistemas. 50](#_Toc389023043)

[PERSONAL PARTICIPANTE 51](#_Toc389023044)

[Auditor Junior 51](#_Toc389023045)

[Reportero 51](#_Toc389023046)

[Encargado de Sistemas. 52](#_Toc389023047)

[Corrector 52](#_Toc389023048)

[Paginador 52](#_Toc389023049)

[CAPÍTULO II: AUDITORÍA INFORMÁTICA 54](#_Toc389023050)

[INSTITUCIÓN: 54](#_Toc389023051)

[Logo: 54](#_Toc389023052)

[Eslogan: 54](#_Toc389023053)

[Direccion: 54](#_Toc389023054)

[Ubicación: 54](#_Toc389023055)

[Reseña Historica: 55](#_Toc389023056)

[Web Site: 55](#_Toc389023057)

[Filosofia Institucional: 55](#_Toc389023058)

[SERVICIOS QUE BRINDA: 55](#_Toc389023059)

[ÁREA INFORMÁTICA. 55](#_Toc389023060)

[Auditoría de sistemas 56](#_Toc389023061)

[ORIGEN DE LA AUDITORIA 56](#_Toc389023062)

[OBJETIVOS Y ALCANCE 56](#_Toc389023063)

[OBJETIVO GENERAL 56](#_Toc389023064)

[OBJETIVOS ESPECIFICOS 56](#_Toc389023065)

[ENFOQUE A UTILIZAR 56](#_Toc389023066)

[DOCUMENTOS A SOLICITAR 57](#_Toc389023067)

[ORGANIGRAMA 57](#_Toc389023068)

[RELACION DE FUNCIONARIOS DEL AREA A EXAMINAR 57](#_Toc389023069)

[TIPO DE SOFTWARE A UTILIZAR 58](#_Toc389023070)

[CERTERO PCAUDITOR 58](#_Toc389023071)

[INFORMES 62](#_Toc389023072)

[Equipos de Cómputo: 62](#_Toc389023073)

[Cuantos equipos existen 63](#_Toc389023074)

[PUNTOS DEBILES Y AMENAZAS. 63](#_Toc389023075)

[MATRIZ FODA(PROPUESTA) 63](#_Toc389023076)

[RECOMENDACIONES DE LA AUDITORIA 64](#_Toc389023077)

[CONEXIONES ELÉCTRICAS 64](#_Toc389023078)

[PUNTOS DÉBILES Y AMENAZAS. 64](#_Toc389023079)

[RECOMENDACIONES 64](#_Toc389023080)

[CABLEADO ESTRUCTURADO. 65](#_Toc389023081)

[NORMA TIA/EIA-568-B 65](#_Toc389023082)

[Objetivos 65](#_Toc389023083)

[PUNTOS DÉBILES Y AMENAZAS. 65](#_Toc389023084)

[RECOMENDACIONES 65](#_Toc389023085)

[CONEXIONES DE REDES 66](#_Toc389023086)

[Puntos débiles y amenazas 66](#_Toc389023087)

[LICENCIAMIENTO DEL SOFTWARE 66](#_Toc389023088)

[PUNTOS DÉBILES Y AMENAZAS 66](#_Toc389023089)

[RECOMENDACIONES 66](#_Toc389023090)

[PLANES DE CONTINGENCIA 66](#_Toc389023091)

[NORMAS PARA USO DE LAS SALAS DE SISTEMAS 67](#_Toc389023092)

[PUNTOS DÉBILES Y AMENAZAS 71](#_Toc389023093)

[Bases de datos, propietarios de la información y usuarios de la misma. 72](#_Toc389023094)

[Propietarios de la información 72](#_Toc389023095)

[Usuarios de la base de datos 72](#_Toc389023096)

[Procedimientos y políticas en caso de desastre 73](#_Toc389023097)

[OBJETIVOS GENERALES Y ESPECÍFICOS 73](#_Toc389023098)

[Generales: 73](#_Toc389023099)

[Específicos: 73](#_Toc389023100)

[ALCANCE 73](#_Toc389023101)

[Acciones a ser consideradas: 73](#_Toc389023102)

[Plan de Prevención 74](#_Toc389023103)

[Plan de Ejecución 74](#_Toc389023104)

[Plan de Recuperación 74](#_Toc389023105)

[Plan de Pruebas 74](#_Toc389023106)

[METODOLOGÍA 74](#_Toc389023107)

[Organización del Plan de Contingencia 75](#_Toc389023108)

[Identificación y Priorización de Riesgos 75](#_Toc389023109)

[Elaboración de los Planes de Contingencia 75](#_Toc389023110)

[Definición y ejecución del plan de pruebas 75](#_Toc389023111)

[Implementación del Plan de Contingencia 76](#_Toc389023112)

[DESARROLLO DE LAS FASES, ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS 76](#_Toc389023113)

[Identificación y Priorización de Riesgos 76](#_Toc389023114)

[Sistemas propios y/o legalidad de los mismos. 81](#_Toc389023115)

[Pruebas Sustantivas 81](#_Toc389023116)

[INFORME DE AUDITORIA 83](#_Toc389023117)

[AUDITORIA DE LA OFIMATICA 84](#_Toc389023118)

[INFORME DE AUDITORIA 87](#_Toc389023119)

[AUDITORIA A LOS SISTEMAS DE REDES 89](#_Toc389023120)

[INFORME DE AUDITORIA 94](#_Toc389023121)

[CONCLUSIONES 95](#_Toc389023122)

[INFORME FINAL DE AUDITORIA 96](#_Toc389023123)

[RESULTADOS 96](#_Toc389023124)

[RESUMEN DE NO CONFORMIDADES 97](#_Toc389023125)

[AREAS DE OPORTUNIDAD O DE MEJORA 97](#_Toc389023126)

CAPITULO I

INVESTIGACIÓN

PRELIMINAR

# CAPÍTULO I: INVESTIGACIÓN PRELIMINAR

## CONSIDERACIONES PREVIAS

Cada día son más las empresas que perciben su información como el motor del negocio que es, un activo estratégico que diariamente es sometido a nuevos y más graves riesgos imposibilitando que de manera efectiva, la información aporte el valor que tiene, siendo necesario vencer la inseguridad y la desconfianza que esto genera. Virus, hackers, averías, incendios, personal descontento, errores humanos, son miles las amenazas que tienen efectos devastadores, y que generan:

* Indisponibilidad: No poder acceder a la información cuando es vital y necesaria para la toma de decisiones, por inoperatividad de las infraestructuras tecnológicas.
* Falta de confidencialidad: Información accedida por personas no autorizadas. Robo de datos de clientes, espionaje, filtraciones, fraude.
* Pérdida de integridad: alteración de la información intencionada o por error al no existir controles.
* Falta de confianza en las transacciones electrónicas con terceros, al no existir mecanismos de autenticidad y repudio.

Afrontar estas situaciones, controlando la inseguridad de nuestros sistemas de información dentro de límites aceptables por el negocio sólo es posible mediante la integración de medidas organizativas y técnicas en el marco del desarrollo de una Cultura de la Seguridad y Calidad de la Información en la empresa.

No es posible eliminar las amenazas pero sí debemos reducir la posibilidad de que actúen y el perjuicio que pueden ocasionar: Es decir, controlar el riesgo para generar seguridad y confianza, aportando veracidad y calidad a la información que se está tratando.

En una sociedad en la que los cambios se producen de manera vertiginosa, y donde la información, la tecnología y su continua innovación son el propulsor principal de una espiral de oportunidades, nuevos riesgos amenazan permanentemente a las organizaciones: la complejidad de la tecnología, información de deficiente calidad, confidencialidad comprometida etc., cuyos efectos son cada vez más graves: pérdida de confianza y oportunidad, costes económicos...

Por ello es necesario proteger la información de las organizaciones y la confianza de sus clientes ayudando al desarrollo de una verdadera cultura de la seguridad en la empresa, desarrollar un proceso de mejora continua y maduración, a través de la evaluación, metodologías de calidad, la auditoría Informática y ayudar a las empresas en el cumplimiento de las normativas.

Actualmente todas las entidades que realizan software comienzan a prestar una gran atención en la calidad y seguridad de sus productos. Esto se debe, en parte, a que los clientes cada vez son más exigentes. Además, el no tener calidad y seguridad, implica la pérdida de clientes puesto que acudirán a aquellas empresas que les ofrezcan una calidad especificada por alguna norma y una seguridad a su producto.

La calidad pretende obtener el cumplimiento de las expectativas pactadas con el/los cliente/s siguiendo los estándares establecidos para garantizar así el éxito.

La calidad depende fundamentalmente de las expectativas de los clientes, ya que son ellos quienes finalmente perciben o evalúan la calidad. Bajo este prisma, la calidad puede ser definida como la brecha entre el desempeño real y el desempeño esperado. A menor brecha, mayor calidad.

Para lograr una buena calidad, es decir para que el desempeño del producto o servicio sea mayor o igual que las expectativas de los clientes, la clave está en conocer y comprender cuáles son esas expectativas.

El principal impacto de una mala calidad es la pérdida de rentabilidad y competitividad. Toda empresa que logra un buen nivel de calidad logra aumentar el valor de sus productos, sus ventas y su participación de mercado. Si además logra reducir sus costos, entonces la competitividad de la empresa será aún mayor.

Los datos de alta calidad deben ser completos, consistentes, exactos y actualizados. La necesidad de este tipo de datos es cada vez mayor ya que las compañías cada vez necesitan ser más eficientes en su operativa, cumplir con las normativas vigentes y contar con capacidades de monitorización que permitan que la calidad de datos se gestione como una iniciativa global.

La calidad comienza con una decisión estratégica que sólo puede ser tomada por la alta gerencia, la cual, es la decisión de competir como una compañía de categoría mundial. La calidad se concentra en lograr un desempeño de alta calidad en cada una de las facetas de la empresa.

La Seguridad informática no comprende únicamente características técnicas, sino que tiene que incorporar al personal, tanto interno como externo, a la gestión y a la organización.

Debido a la sensación de inseguridad que planea sobre la sociedad en general, también en el campo de la informática se requiere cada vez más un aumento de los niveles de Seguridad por parte de todos.

La Auditoría de Sistemas de Información comprende la revisión y la evaluación independiente y objetiva, abarcando todo o algunas de las áreas de los sistemas de información, sus estándares y procedimientos en vigor, para determinar si el sistema salvaguarda los activos, mantiene la integridad de la información y el cumplimiento de los objetivos fijados por la organización.

Teniendo en cuenta lo mencionado anteriormente, se puede observar la importancia de la Calidad y Seguridad en los entornos informáticos.

De esta importancia surge este proyecto, cuya finalidad es profundizar en el conocimiento de la calidad y de la seguridad de la información.

Se trata de relacionar ambas características, a la luz de los principales estándares aplicables, así como la auditoría como herramienta para las revisiones.

Se busca desarrollar una cultura de calidad y seguridad.

Se tratan los conceptos de calidad, seguridad y auditoría informática. La aplicación de estándares para su puesta en marcha y se dan detalles sobre su contenido. Con todo esto se pretende dar al lector un conocimiento más amplio de aquellas normas que afectan directamente a la calidad, a la seguridad y a la auditoría informática, que le permita saber que norma aplicar.

Se profundiza en estos conceptos, aplicándolos a las empresas y a la situación actual del mercado, evaluando las tendencias de la seguridad, auditoría y calidad en un futuro. Se puede observar la importancia de estos términos.

Además se le da gran importancia a la auditoría informática relacionada con la calidad y la seguridad.

El fin último es que cada persona implicada en labores informáticas esté convencida de que un trabajo bien hecho es aquel que cumple los requisitos de calidad y de seguridad necesarios, no sólo cuando ya está finalizado, sino durante toda su ejecución.

## PLANEACIÓN DE LA AUDITORÍA

PLANEACION DE

LA AUDITORIA

### Revisión Detallada

Pasos para la revisión detallada:

**A nivel organizacional.**

1. Objetivos a corto y largo plazo.
2. Misión, Visión y Valores.
3. Antecedentes de la empresa
4. Organigrama
5. Función de cada uno de los departamentos.
6. Relaciones entre las diversas áreas del negocio
7. Políticas Generales.

**A nivel del área de informática:**

1. Manual de Funciones (Fichas ocupacionales).
2. Manual de políticas, reglamentos internos y lineamientos generales.
3. Número de personas y puestos en el área.
4. Procedimientos administrativos del área.
5. Presupuestos y costos del área.

**RECURSOS MATERIALES Y TÉCNICOS:**

1. Solicitar documentos sobre los equipos, así como el número de ellos, su localización y sus características (de los equipos instalados, por instalar y programados).
2. Estudio de viabilidad.
3. Fechas de instalación de los equipos y planes de instalación.
4. Contratos vigentes de compra, renta y servicio de mantenimiento.
5. Contratos de seguros.
6. Convenios que se tienen con otras instalaciones.
7. Configuración de los equipos y capacidades actuales y máximas.
8. Configuración de equipos de comunicación(redes internas y externas) y localización de los equipos.
9. Planes de expansión.
10. Ubicación general de los equipos.
11. Políticas de operación.
12. Políticas del uso de los equipos.
13. Políticas de seguridad física y prevención contra contingencias internas y externas.

**sistemas:**

1. Descripción general de los sistemas instalados y de los que estén por instalarse.
2. Manual de procedimientos de los sistemas.
3. Descripción genérica.
4. Diagramas de entrada, archivos, salidas.
5. Fecha de instalación de los sistemas.
6. Proyecto de instalación de nuevos sistemas.
7. Bases de datos, propietarios de la información y usuarios de la misma.
8. Procedimientos y políticas en caso de desastre.
9. Sistemas propios y/0 legalidad de los mismos.

### Pruebas de Controles de los Usuarios

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

### Pruebas Sustantivas

1. Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.
2. Pruebas para asegura la calidad de los datos.
3. Pruebas para identificar la inconsistencia de los datos.
4. Pruebas para comparar con los datos o contadores físicos.
5. Confirmación de datos con fuentes externas.
6. Pruebas para confirmar la adecuada comunicación.
7. Pruebas para determinar la falta de seguridad.
8. Pruebas para determinar problemas de legalidad.

### Examen y Evaluación de la Información

**EVALUACIÓN DE SISTEMAS**

La elaboración de sistemas debe ser evaluada con mucho detalle, para lo cual se debe revisar si existen realmente sistemas entrelazados como un todo o bien si existen programas aislados. Otro de los factores a evaluar es si existe un plan estratégico para la elaboración de los sistemas o si se están elaborados sin el adecuado señalamiento de prioridades y de objetivos.

El plan estratégico deberá establecer los servicios que se presentarán en un futuro contestando preguntas como las siguientes:

1. ¿Cuáles servicios se implementarán?
2. ¿Cuándo se pondrán a disposición de los usuarios?
3. ¿Qué características tendrán?
4. ¿Cuántos recursos se requerirán?

La estrategia de desarrollo deberá establecer las nuevas aplicaciones, recursos y la arquitectura en que estarán fundamentados:

1. ¿Qué aplicaciones serán desarrolladas y cuando?
2. ¿Qué tipo de archivos se utilizarán y cuando?
3. ¿Qué bases de datos serán utilizarán y cuando?
4. ¿Qué lenguajes se utilizarán y en que software?
5. ¿Qué tecnología será utilizada y cuando se implementará?
6. ¿Cuantos recursos se requerirán aproximadamente?
7. ¿Cuál es aproximadamente el monto de la inversión en hardware y software?

En lo referente a la consulta a los usuarios, el plan estratégico debe definir los requerimientos de información de la dependencia.

1. ¿Qué estudios van a ser realizados al respecto?
2. ¿Qué metodología se utilizará para dichos estudios?
3. ¿Quién administrará y realizará dichos estudios?

En el área de auditoría interna debe evaluarse cuál ha sido la participación del auditor y los controles establecidos.

Por último, el plan estratégico determina la planeación de los recursos.

1. ¿Contempla el plan estratégico las ventajas de la nueva tecnología?
2. ¿Cuál es la inversión requerida en servicios, desarrollo y consulta a los usuarios?

El proceso de planeación de sistemas deberá asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos. Estos recursos (hardware, software y comunicaciones) deberán ser compatibles con la arquitectura y la tecnología, conque se cuenta actualmente.

Los sistemas deben evaluarse de acuerdo con el ciclo de vida que normalmente siguen: requerimientos del usuario, estudio de factibilidad, diseño general, análisis, diseño lógico, desarrollo físico, pruebas, implementación, evaluación, modificaciones, instalación, mejoras. Y se vuelve nuevamente al ciclo inicial, el cual a su vez debe comenzar con el de factibilidad.

La primera etapa a evaluar del sistema es el estudio de factibilidad, el cual debe analizar si el sistema es factible de realizarse, cuál es su relación costo/beneficio y si es recomendable elaborarlo.

Se deberá solicitar el estudio de factibilidad de los diferentes sistemas que se encuentren en operación, así como los que estén en la fase de análisis para evaluar si se considera la disponibilidad y características del equipo, los sistemas operativos y lenguajes disponibles, la necesidad de los usuarios, las formas de utilización de los sistemas, el costo y los beneficios que reportará el sistema, el efecto que producirá en quienes lo usarán y el efecto que éstos tendrán sobre el sistema y la congruencia de los diferentes sistemas.

En el caso de sistemas que estén funcionando, se deberá comprobar si existe el estudio de factibilidad con los puntos señalados y compararse con la realidad con lo especificado en el estudio de factibilidad

Por ejemplo en un sistema que el estudio de factibilidad señaló determinado costo y una serie de beneficios de acuerdo con las necesidades del usuario, debemos comparar cual fue su costo real y evaluar si se satisficieron las necesidades indicadas como beneficios del sistema.

Para investigar el costo de un sistema se debe considerar, con una exactitud razonable, el costo de los programas, el uso de los equipos (compilaciones, programas, pruebas, paralelos), tiempo, personal y operación, cosa que en la práctica son costos directos, indirectos y de operación.

Los beneficios que justifiquen el desarrollo de un sistema pueden ser el ahorro en los costos de operación, la reducción del tiempo de proceso de un sistema. Mayor exactitud, mejor servicio, una mejoría en los procedimientos de control, mayor confiabilidad y seguridad.

### EVALUACIÓN DEL ANÁLISIS

En esta etapa se evaluarán las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis.

Se deberá evaluar la planeación de las aplicaciones que pueden provenir de tres fuentes principales:

1. La planeación estratégica: agrupadas las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la dependencia, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.
2. Los requerimientos de los usuarios.
3. El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.

La situación de una aplicación en dicho inventario puede ser alguna de las siguientes:

1. Planeada para ser desarrollada en el futuro.
2. En desarrollo.
3. En proceso, pero con modificaciones en desarrollo.
4. En proceso con problemas detectados.
5. En proceso sin problemas.
6. En proceso esporádicamente.

Nota: Se deberá documentar detalladamente la fuente que generó la necesidad de la aplicación. La primera parte será evaluar la forma en que se encuentran especificadas las políticas, los procedimientos y los estándares de análisis, si es que se cumplen y si son los adecuados para la dependencia.

Es importante revisar la situación en que se encuentran los manuales de análisis y si están acordes con las necesidades de la dependencia. En algunas ocasiones se tiene una microcomputadora, con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una dependencia específica.

Se debe evaluar la obtención de datos sobre la operación, flujo, nivel, jerarquía de la información que se tendrá a través del sistema. Se han de comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

La auditoría en sistemas debe evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse.

Con la información obtenida podemos contestar a las siguientes preguntas:

1. ¿Se está ejecutando en forma correcta y eficiente el proceso de información?
2. ¿Puede ser simplificado para mejorar su aprovechamiento?
3. ¿Se debe tener una mayor interacción con otros sistemas?
4. ¿Se tiene propuesto un adecuado control y seguridad sobre el sistema?
5. ¿Está en el análisis la documentación adecuada?

### EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA

En esta etapa se deberán analizar las especificaciones del sistema.

¿Qué deberá hacer?, ¿Cómo lo deberá hacer?, ¿Secuencia y ocurrencia de los datos, el proceso y salida de reportes?

Una vez que hemos analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los controles y la determinación de los procedimientos de operación y decisión.

Al tener el análisis del diseño lógico del sistema debemos compararlo con lo que realmente se está obteniendo en la cual debemos evaluar lo planeado, cómo fue planeado y lo que realmente se está obteniendo.

Los puntos a evaluar son:

1. Entradas.
2. Salidas.
3. Procesos.
4. Especificaciones de datos.
5. Especificaciones de proceso.
6. Métodos de acceso.
7. Operaciones.
8. Manipulación de datos (antes y después del proceso electrónico de datos).
9. Proceso lógico necesario para producir informes.
10. Identificación de archivos, tamaño de los campos y registros.
11. Proceso en línea o lote y su justificación.
12. Frecuencia y volúmenes de operación.
13. Sistemas de seguridad.
14. Sistemas de control.
15. Responsables.
16. Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

1. Manual del usuario.
2. Descripción de flujo de información y/o procesos.
3. Descripción y distribución de información.
4. Manual de formas.
5. Manual de reportes.
6. Lista de archivos y especificaciones.

Lo que se debe determinar en el sistema:

En el procedimiento:

1. ¿Quién hace, cuando y como?
2. ¿Qué formas se utilizan en el sistema?
3. ¿Son necesarias, se usan, están duplicadas?
4. ¿El número de copias es el adecuado?
5. ¿Existen puntos de control o faltan?

En la gráfica de flujo de información:

1. ¿Es fácil de usar?
2. ¿Es lógica?
3. ¿Se encontraron lagunas?
4. ¿Hay faltas de control?

En el diseño:

1. ¿Cómo se usará la herramienta de diseño si existe?
2. ¿Qué también se ajusta la herramienta al procedimiento?

### EVALUACIÓN DEL DESARROLLO DEL SISTEMA

En esta etapa del sistema se deberán auditar los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema.Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. De ese modo contará con los mejores elementos para una adecuada toma de decisiones.Al tener un proceso distribuido, es preciso considerar la seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, los tipos de mensajes requeridos, el trafico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza.Las características que deben evaluarse en los sistemas son:

1. Dinámicos (susceptibles de modificarse).
2. Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo)
3. Integrados (un solo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
4. Accesibles (que estén disponibles).
5. Necesarios (que se pruebe su utilización).
6. Comprensibles (que contengan todos los atributos).
7. Oportunos (que esté la información en el momento que se requiere).
8. Funcionales (que proporcionen la información adecuada a cada nivel).
9. Estándar (que la información tenga la misma interpretación en los distintos niveles).
10. Modulares (facilidad para ser expandidos o reducidos).
11. Jerárquicos (por niveles funcionales).
12. Seguros (que sólo las personas autorizadas tengan acceso).
13. Únicos (que no duplique información).

### CONTROL DE PROYECTOS

**CUESTIONARIO**

**1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?**

No existe como tal. Los proyectos surgen a partir de alguna nueva necesidad que se tenga dentro del Independiente de Hidalgo y las fechas son asignadas por el gerente administrativo.  
**2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?**

-  
**3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?**

-  
**4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?**

-  
**5. Escribir la lista de proyectos a corto plazo y largo plazo.**

Proyectos a corto plazo:

* Sistema tarificador.
* Sistema de tickets para quejas.
* Sistema para control de inventarios de accesorios de motocicletas.

Proyectos a largo plazo:

* Sistema basado en web para atención a clientes.
* Chat con posibilidades de intercambio de archivos para uso interno.
* Aplicación móvil (plataforma android) de El Independiente de Hidalgo.
* Aplicación móvil (plataforma iOS) de El Independiente de Hidalgo.

**6. Escribir una lista de sistemas en proceso periodicidad y usuarios.**

La tabla siguiente representa una lista de sistemas de información que están en proceso:

|  |  |  |
| --- | --- | --- |
| Proyecto | Periodicidad | Usuarios |
| Sistema de control de inventarios de accesorios de motocicletas. | Cada semana. | Personal de circulación. |
| Sistema tarificador. | Cada semana. | Personal administrativo. |
| Sistema de tickets para quejas. | Cada tercer día. | Recepcionista. |
| Aplicación móvil para Android. | Cada mes. | Suscriptores. |
| Aplicación móvil para iOS. | Cada mes. | Suscriptores. |

**7. ¿Quién autoriza los proyectos?**

Los proyectos son autorizados por el gerente general Ángel Sánchez Cartagena.  
**8. ¿Cómo se asignan los recursos?**

La asignación de los recursos se lleva a cabo en reuniones con el gerente general,   
**9. ¿Cómo se estiman los tiempos de duración?**

La estimación de los tiempos de duración es dada al evaluarse la prioridad que tengan estos, es decir, si la empresa requiere de una aplicación o una solución a algún problema, los tiempos de asignación son considerablemente rápidos, mientras que, al ser proyectos grandes o de mayor importancia para la empresa, a estos se les asignan periodos largos, como de 2 a 3 meses.  
**10. ¿Quién interviene en la planeación de los proyectos?**

En la planeación de los proyectos, a veces intervienen los usuarios que ocuparán algún sistema, o bien pueden llegar a intervenir terceros que representen compañías si es que se llegase a trabajar en conjunto con alguna otra dependencia.  
**11. ¿Cómo se calcula el presupuesto del proyecto?**

Mediante una junta directiva con el gerente general, el director del Independiente de Hidalgo y el jefe del área de sistemas, se llegan a acuerdos para proponer un presupuesto para proyectos grandes y robustos que requieran de una inversión monetaria considerable.

**12. ¿Qué técnicas se usan en el control de los proyectos?**

Como tal, no existen técnicas para el control de los proyectos, pero el desarrollador de sistemas lleva un control de versiones en el servidor local del independiente.   
**13. ¿Quién asigna las prioridades?**

Las prioridades son asignadas por el gerente general del periódico.  
**14. ¿Cómo se asignan las prioridades?**

Las prioridades son asignadas de acuerdo al grado de importancia y necesidad de cada punto del proyecto a desarrollar.  
**15. ¿Cómo se controla el avance del proyecto?**

El avance del proyecto se controla mediante un control de versiones.  
**16. ¿Con qué periodicidad se revisa el reporte de avance del proyecto?**

No existe un periodo para revisar reportes de avance del proyecto; sin embargo, al realizar un proyecto grande o mediano, se revisan frecuentemente los avances que se tengan de dicho proyecto.  
**17. ¿Cómo se estima el rendimiento del personal?**

No existen medidas para estimar el rendimiento del personal.  
**18. ¿Con que frecuencia se estiman los costos del proyecto para compararlo con lo presupuestado?**

Se estiman cada que existe un avance del proyecto a desarrollar.  
**19. ¿Qué acciones correctivas se toman en caso de desviaciones?**

**Se aplican reingenierías o bien reprogramación de lo desarrollado.  
20. ¿Qué pasos y técnicas siguen en la planeación y control de los proyectos?**Enumérelos secuencialmente.   
( ) Determinación de los objetivos.   
( ) Señalamiento de las políticas.   
(X) Designación del funcionario responsable del proyecto.   
(X) Integración del grupo de trabajo.   
( ) Integración de un comité de decisiones.   
( ) Desarrollo de la investigación.   
( ) Documentación de la investigación.   
(X) Factibilidad de los sistemas.   
(X) Análisis y valuación de propuestas.   
( ) Selección de equipos.

**21. ¿Se llevan a cabo revisiones periódicas de los sistemas para determinar si aún cumplen con los objetivos para los cuales fueron diseñados?**De análisis SÍ ( ) NO ( X )   
De programación SÍ ( X ) NO ( ) **Observaciones   
22. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual.**

|  |  |
| --- | --- |
| Proyecto | Plazo aproximado |
| Sistema de control de inventarios de accesorios de motocicletas. | 1 mes. |
| Sistema tarificador. | 1 mes. |
| Sistema de tickets para quejas. | 2 meses. |
| Aplicación móvil para Android. | 8 meses. |
| Aplicación móvil para iOS. | 8 meses. |
| Sistema basado en web para atención a clientes. | 8 meses. |
| Chat con posibilidades de intercambio de archivos para uso interno. | 12 meses. |

**CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN**

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación. Las revisiones se efectúan en forma paralela desde el análisis hasta la programación y sus objetivos son los siguientes:

ETAPA DE ANÁLISIS Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

ETAPA DE DISEÑO Descubrir errores, debilidades, omisiones antes de iniciar la codificación.

ETAPA DE PROGRAMACIÓN Buscar la claridad, modularidad y verificar con base en las especificaciones.

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan: si se descubren en el momento de programación será más alto que si se detecta en la etapa de análisis. Esta función tiene una gran importancia en el ciclo de evaluación de aplicaciones de los sistemas de información y busca comprobar que la aplicación cumple las especificaciones del usuario, que se haya desarrollado dentro de lo presupuestado, que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

### Control de diseño de sistemas y programación

Los sistemas de Información que son desarrollados para su uso en El Independiente de Hidalgo, tiene la característica de ser creados “in-house” debido a ser sistemas a medida. Los requerimientos de dichos sistemas están definidos por los usuarios operadores, sin embargo, quien da pauta o pie a que se inicie un proyecto de software son el consejo directivo.

A continuación se presenta el cuestionario que evalúa el diseño y prueba de los sistemas:

**1. ¿Quiénes intervienen al diseñar un sistema?**

* Usuario.
* Analista.
* Programadores.
* Operadores.
* Gerente de departamento.
* Auditores internos.
* Asesores.
* Otros.

**2. ¿Los analistas son también programadores?**

SÍ (x) NO ( )

**3. ¿Qué lenguaje o lenguajes conocen los analistas?**

Java y Delphi

**4. ¿Cuántos analistas hay y qué experiencia tienen?**

1, 5 años

**5. ¿Qué lenguaje conocen los programadores?**

Delphi, C++

**6. ¿Cómo se controla el trabajo de los analistas?**

Verificando el cumplimiento/avance en tiempo y forma de objetivos de proyectos de software

**7. ¿Cómo se controla el trabajo de los programadores?**

Verificando el cumplimiento/avance en tiempo y forma de objetivos de proyectos de software

**8. Indique qué pasos siguen los programadores en el desarrollo de un programa:**

• Estudio de la definición ( x)

• Discusión con el analista (x )

• Diagrama de bloques ( )

• Tabla de decisiones ( )

• Prueba de escritorio ( )

• Codificación (x )

• ¿Es enviado a captura o los programadores capturan? ( x)

• ¿Quién los captura?\_\_\_\_\_\_\_\_Programadores\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

• Compilación (x )

• Elaborar datos de prueba ( )

• Solicitar datos al analista ( )

• Correr programas con datos ( x)

• Revisión de resultados (x )

• Corrección del programa ( x)

• Documentar el programa ( x)

• Someter resultados de prueba ( )

• Entrega del programa (x )

**9. ¿Qué documentación acompaña al programa cuando se entrega?**

Manual de usuario

A pesar de contar con controles rigurosos que regulen el flujo de trabajo del diseño de sistemas y su respectiva programación; podemos notar que con un control básico como el anterior es posible llevar una mejor gestión en proyectos de software de El Independiente de Hidalgo.

**INSTRUCTIVOS DE OPERACIÓN**

No aplica.

#### Forma de Implementación

La finalidad de evaluar los trabajos que se realizan para iniciar la operación de un sistema, esto es, la prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema etc.

Indicar cuáles puntos se toman en cuenta para la prueba de un sistema:

Prueba particular de cada programa (**✓**)

Prueba por fase validación, actualización (**✓** )

Prueba integral del paralelo ( )

Prueba en paralelo sistema ( )

Otros (especificar)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### ENTREVISTA A USUARIOS

**1. ¿Considera que el Departamento de Sistemas de Información da los resultados esperados?.-**Si (X) No ( )   
**¿Por que?**

Cumple con los requerimientos que se le piden y da soluciones rápidas.

**2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?**Deficiente ( )   
Aceptable ( )   
Satisfactorio (X)   
Excelente ( )   
**¿Por que?**

Brindan una excelente respuesta ante solicitudes de alteraciones a programas, y tienen un buen soporte técnico.

**3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?**No las cubre ( )   
Parcialmente ( )   
La mayor parte ( )   
Todas (X)   
¿Por que?

Por que realiza todas las funciones que se deben de realizar en el área.

**4. ¿Hay disponibilidad del departamento de cómputo para sus requerimientos?**Generalmente no existe ( )   
Hay ocasionalmente ( )   
Regularmente ( )   
Siempre (X)   
¿Por que? Alteran programas si se necesitan alterarlos para poder cumplir las necesidades del personal.

**5. ¿Son entregados con puntualidad los trabajos?**Nunca ( )   
Rara vez ( )   
Ocasionalmente ( )   
Generalmente (X)   
Siempre ( )   
¿Por que?

Existen algunos pequeños retrasos de vez en cuando, pero generalmente se entregan en tiempo y forma.

**6. ¿Que piensa de la presentación de los trabajadores solicitados al departamento de cómputo?**Deficiente ( )   
Aceptable (X)   
Satisfactorio ( )   
Excelente ( )   
¿Por que? Existe diversificación en perfiles a ciertas área, por tanto los empleados cubren los perfiles que deben de cumplir.

**7. ¿Que piensa de la asesoría que se imparte sobre informática?**No se proporciona ( )   
Es insuficiente ( )   
Satisfactoria (X)   
Excelente ( )   
¿Por que? Al personal nuevo, se le explica el correcto manejo del programa que estos vayan a ocupar y en todo momento existe soporte.

**8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que** **utiliza?**   
Nula ( )   
Riesgosa ( )   
Satisfactoria ( )   
Excelente ()   
Lo desconoce (X)   
¿Por que?

**9. ¿Existen fallas de exactitud en los procesos de información?**

No¿Cuáles?

**10. ¿Cómo utiliza los reportes que se le proporcionan?**

No se han proporcionado reportes

**11. ¿Cuáles no Utiliza?**

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

**13. ¿Que sugerencias presenta en cuanto a la eliminación de reportes modificación, fusión, división de reporte?**

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

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

**16. ¿Que opinión tiene el manual?**NOTA: Pida el manual del usuario para evaluarlo.

Es muy explicativo y agradable cuando se lee, no aburre ni está lleno de texto.

**17. ¿Quién interviene de su departamento en el diseño de sistemas?**

Generalmente interviene el jefe de Sistemas y quienes hacen servicio social o prácticas profesionales.

**18. ¿Que sistemas desearía que se incluyeran?**

Ninguno.

**19. Observaciones:**

Ninguna.

### 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

Por medio del cuestionario anterior es posible determinar si hubo eliminación de información, alterado de datos, duplicado de los mismos, a algún otro evento que resulte perjudicial para El Independiende de Hidalgo, los datos deben estar debidamente protegidos.

#### 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.**

Por fecha (x )

por fecha y hora ( )

por turno de operación ( )

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

Estos controles garantizan que la salida está autorizada, es precisa y está completa, y además que se entregue al personal responsable de ella y que este adecuadamente archivada.

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

**No.**

1. ¿Dónde se encuentran esos locales?

**No hay.**

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

**No hay.**

1. ¿Qué confidencialidad se tiene en esos locales?

**No hay.**

1. ¿Quién entrega los documentos de salida?

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

1. ¿En qué forma se entregan?

**Las banderas se entregan en forma física.**

1. ¿Qué documentos?

**El documento del periódico día.**

1. ¿Qué controles se tienen?

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

1. ¿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.**

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

Destruye ( ) Vende ( ) Tira ( ) Otro **Se Recicla**

#### CONTROL DE MEDIOS 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 (x)
3. (señalar que tipo de protección )\_\_\_Extintores\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Cerradura especial (x )
5. Otra

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

En el SITE del Independiente de Hidalgo se cuenta con 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?**Anteriormente era hasta que el disco duro del servidor llegaba al límite; hoy en día son hasta que el disco duro tiene a lo sumo un 70% de espacio ocupado.

**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? Existen carpetas en el servidor del Independiente que contienen una contraseña, misma que el personal del periódico conoce.

**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) El Independiente de Hidalgo almacena sus copias de seguridad en un disco duro de tipo espejo.

**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 espejo.

**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) 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 más 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 cuál 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.

Como pudimos observar, en El Independiente de Hidalgo no se cuenta con controles que permitan llevar planes de mantenimiento preventivo, el tipo de mantenimiento que se lleva a cabo ahí es de tipo correctivo, es aquí en conde encontramos una oportunidad, y como mejora se tiene la de implementar controles que permitan llevar a cabo mantenimiento preventivo periódicamente.

### 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 semestralmente, con el cambio de prestador 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.

### 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:

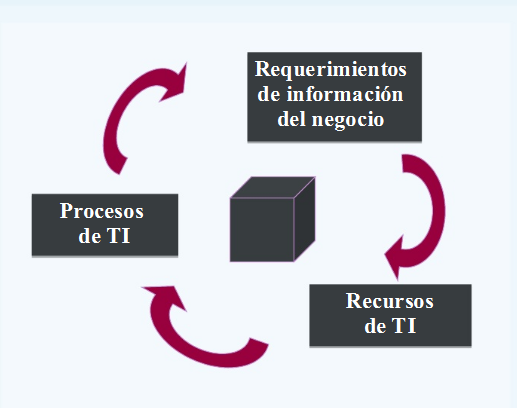
La Tecnología de Información (TI) esté alineada con la misión y visión.

LA TI capacite y maximice los beneficios.

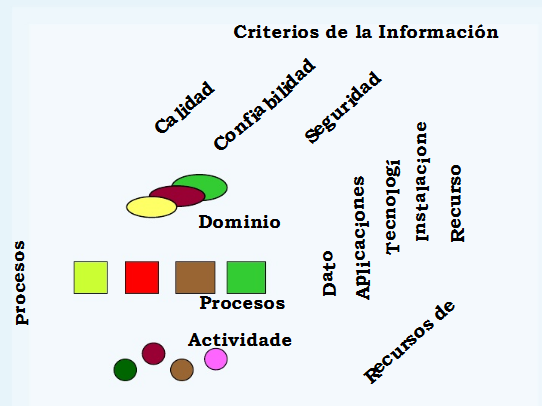
Los recursos de TI sean usados responsablemente.

Los riesgos de TI sean manejados apropiadamente.

COBIT – PRINCIPIOS

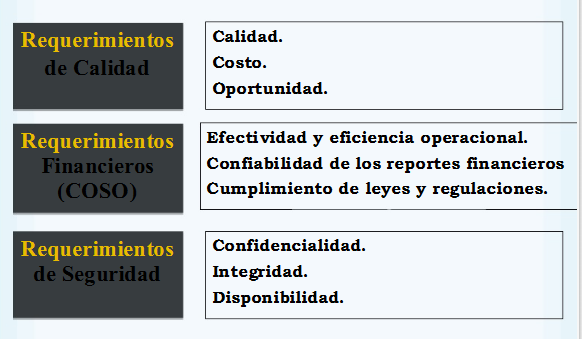


**COBIT – ESTRUCTURA**



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**



## ADMINISTRACIÓN

El Independiente de Hidalgo cuenta con 20 equipos de cómputo, un site y un equipo para mantener el aire acondicionado. La encargada del área de sistemas es la persona quien brindará a cada uno de los integrantes de ésta área el orden que tiene que seguir para poder tener un desempeño óptimo cuando cada uno realice sus actividades encomendadas.

## A NIVEL DEL ÁREA DE INFORMÁTICA

### Objetivos a corto plazo:

Mantener en óptimas condiciones todos los equipos para poder realizar de forma óptima todas las actividades que se llevan a cabo dentro de la empresa, así como que se cumplan todas las necesidades que la empresa pueda tener.

### Objetivos a largo plazo.

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

## RECURSOS MATERIALES Y TECNICOS

### Estudios de viabilidad.

El estudio realizado en este documento tiene como fin el conocer si suficiente viabilidad necesaria para que la auditoría que se realizará muestre que cada uno de los elementos que están integrados en esta unidad sean capaces de poder realizar óptimamente las actividades encomendadas de una forma eficiente.

### Número de equipos, localización y las características

Se cuenta con 20 equipos, de los cuáles:

* 16 son marca Dell, modelo Studio Z, contando con 512 MB de memoria para videos, 2GB de RAM y 160 GB de disco duro.
* 4 son marca Apple, modelo iMac G7, contando con 1 GB de memoria para videos, 8 GB de memoria RAM, 750 GB de disco duro y un procesador Intel Core Dual a 1.8 GHz.

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

### Fechas de instalación de los equipos y planes de instalación.

Los equipos fueron instalados en el mayo del 2011, siendo 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 y procesamiento de la información.

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

La empresa no cuenta con contrato de mantenimiento alguno, pues un personal que está en el área de sistemas es el encargado de dar mantenimiento preventivo y correctivo a los equipos de cómputo de El Independiente de Hidalgo.

### Contratos de seguros.

Ninguno.

### Convenios que se tienen con otras instalaciones.

Ninguno.

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

El equipo de cómputo de la empresa cuenta con una configuración básica gracias al fin con el que éstos son utilizados. Únicamente es necesario que tengan acceso a internet y que también se tenga instalada la paquetería de Microsoft Office, siendo esto un requisito para los reporteros y correctores.

En cambio, el encargado de sistemas, diseñadores y paginadores, requieren de equipos con capacidades superiores dado a las necesidades que tienen día con día, y dado a los requisitos que exigen el software que utilizan a diario. Para ello, se cuentan con equipos iMac G7, facilitándoles éstas tareas gracias a la arquitectura que tienen estos equipos.

### Planes de expansión.

El Independiente de Hidalgo no cuenta con plan de expansión alguno.

### Ubicación general de los equipos.

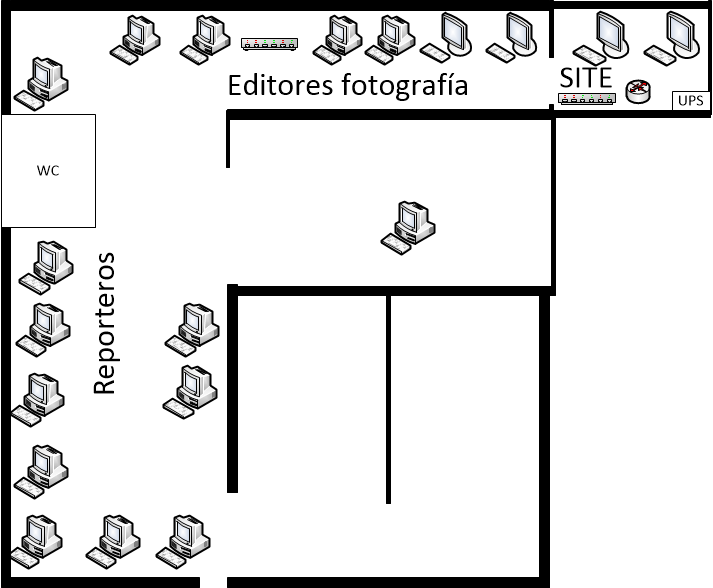


Figura 1. Ubicación de los equipos de cómputo en El Independiente de Hidalgo.

### Políticas de operación.

El Independiente de Hidalgo no cuenta con políticas de operación escritas, sin embargo, el personal tiene en claro que el centro sí opera con algunas políticas como lo son el pasar las notas con la inicial del nombre del reportero o imprimir sus guías para que los paginadores se encarguen de contemplar el espacio que usarán para la nota.

### Políticas de uso de los equipos.

El personal que utiliza el equipo de cómputo de la empresa tiene prohibido acceder a redes sociales tales como Facebook, Twitter, Youtube, Google Plus, entre otras, dado a que además de incentivar a los empleados a malgastar su tiempo en actividades no correspondientes a las que les pertenecen, reducen drásticamente el ancho de banda de la empresa, mismo que es de vital importancia mantenerlo en su máxima capacidad, pues la empresa no ha contratado un paquete de banda ancha superior.

## SISTEMAS

### Manual de procedimientos de los sistemas.

El Independiente de Hidalgo no cuenta con un manual de procedimientos de los sistemas, sin embargo, el equipo de auditores HConsultores propone el siguiente:

**Logotipo:**



Figura 1. : Logotipo a utilizar en los sistemas.

**Nombre oficial de la institución:** El independiente de Hidalgo.

**Introducción:** El presente manual permitirá conocer a fondo el funcionamiento de ésta unidad, permitiendo así conocer el funcionamiento interno y así auxiliar a la capacitación de personal nuevo y del existente, pues se describen 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.

### Descripción genérica.

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

**Creación de la nota por parte de los reporteros.**

**La persona encargada de la sección internacional** se encarga de buscar a través de distintas fuentes las noticias más relevantes durante el día, para después ser seleccionadas y así ser publicadas.

**Los corresponsales** se encargan de enviar sus notas a uno de los reporteros para que ellos las seleccionen y le sean brindados los avances a los correctores y después a los paginadores.

Después se imprimen las guías que contienen las notas que pasarán a ser publicadas, para que **los paginadores y la persona encargada de fotografía** busquen imágenes que permitan ilustrar la nota.

**La directora del periódico** entonces ha armado la guía de cómo se armará el periódico. Esta guía es enviada entonces al **encargado del área de sistemas**.

**La persona encargada de fotografía**, se encarga de enviar la imagen con la que se ilustrará la nota a los paginadores.

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

Entonces, 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 se encargue de subir las notas finales a la página web y también para que se cree la versión digital del periódico.

### Diagramas de entrada, archivos, salida.

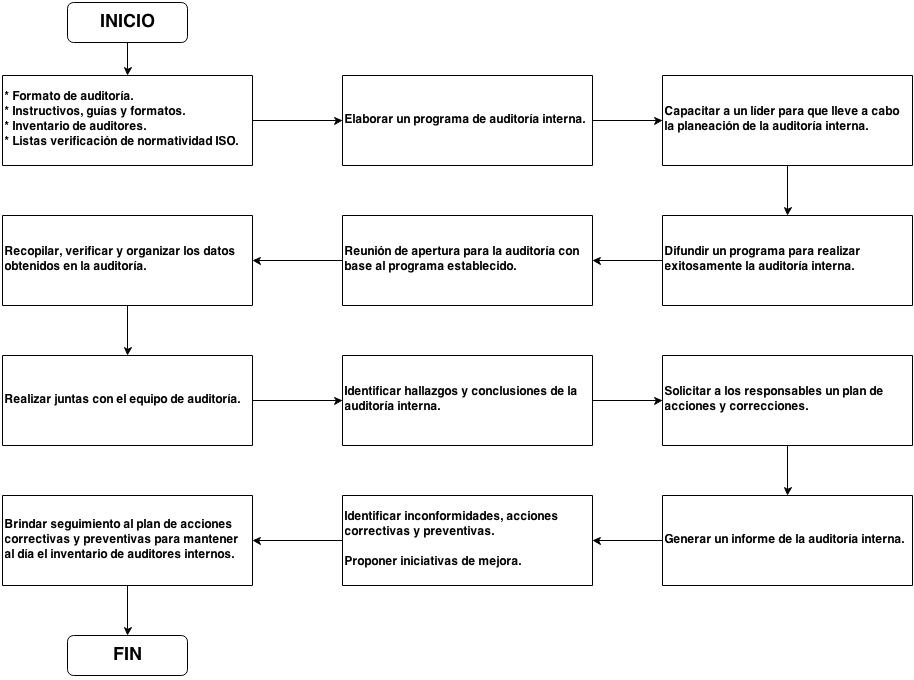


Figura 1. Diagramas de entrada, archivos, salida

### 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:

### Auditor Junior

**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, manejo de sistemas operativos Linux.

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:

### Reportero

**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.

### Encargado de Sistemas.

**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.

### Corrector

**Puesto:** Corrector

**Estudios:** Licenciado en Comunicación.

**Experiencia:** 6 meses como reportero en periódico el Independiente

Buena presentación

**Sueldo:** $1500 y prestaciones de ley.

### Paginador

**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 Adobe Photoshop, Adobe Indesign, Adobe Flash.

Buena presentación

**Sueldo:** $5500 y prestaciones de ley.

CAPITULO II

AUDITORIA

INFORMÁTICA

# CAPÍTULO II: AUDITORÍA INFORMÁTICA

## INSTITUCIÓN:

El independiente de Hidalgo

### Logo:



Figura 2. Logotipo a utilizar en los sistemas.

### Eslogan:

*Libre por convicción*

### Direccion:

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

### Ubicación:

****

Figura 2. Ubicación

### Reseña Historica:

El 15 de abril de 2009 salió a la luz pública el periódico El Independiente de Hidalgo, con una línea libre, crítica, veraz, ética e independiente y con la misión de contribuir al progreso de la sociedad Hidalguense. La línea editorial se define como plural, responsable, participativa en el ámbito informativo; con equidad de género, partidista, ideológica, y de culto, siempre en busca de todas las versiones de los hechos, así como la defensa de las clases marginadas y desprotegidas, siempre preservando la libre expresión y la libertad de prensa. El consejo Editorial está conformado por cinco miembros destacando en los ámbitos culturales, tanto de investigación, docencia, empresarial y principalmente en el periodístico.

### Web Site:

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

### Filosofia Institucional:

Somos periodistas responsables encargados de llevar la información hacia el público en general con la finalidad de satisfacer su necesidad de saber qué es lo que ocurre en los principales municipios del estado de hidalgo. Todos nuestros colaboradores tendrán la libertad absoluta para expresar sus ideas, siempre y cuando se ciñan a los principios legales y de la práctica periodística que aquí se señala. Este Diario es un foro abierto a todas las ideas, pero no a la práctica de intereses personales o de grupo que atenten contra los derechos y garantías fundamentales consagradas en la Constitución. Los colaboradores serán altamente responsables de sus opiniones; como medio, mantendremos el respeto a la libertad de expresión, siempre y cuando no se atente contra la dignidad de las personas mencionadas en nuestras publicaciones. Los periodistas de El Independiente de Hidalgo entendemos con claridad que los funcionarios e integrantes de los gobiernos federal, estatal, y municipal están obligados a cumplir con la rendición de cuentas de sus actos frente de los puestos públicos encomendados y evitar que sus actividades privadas afecten las funciones públicas, por lo que el límite del trabajo periodístico será la frontera que pongan estos servidores para que su vida privada no trascienda y afecte al erario y a la sociedad.

### SERVICIOS QUE BRINDA:

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.

### ÁREA INFORMÁTICA.

El área de sistemas está conformada por una red de tipo estrella, mediante la cual se comparte la información de los reporteros, con los correctores, los paginadores y fotografía. En total son 20 equipos de cómputo, todos de escritorio, de los cuáles 4 son equipos MAC ocupados por los trabajadores de diseño y paginación.

## Auditoría de sistemas

### ORIGEN DE LA AUDITORIA

La presente Auditoria se realiza en cumplimiento del Plan de Estudio que se tiene previsto para el periodo de Enero-Junio del 2014 en el periódico El Independiente de Hidalgo, aprobada mediante Plan de Estudios Auditoria Informática para la Licenciatura en Sistemas Computacionales.

Asesor: Licenciada en Sistemas Computacionales Adriana Katia López Hernández.

### OBJETIVOS Y ALCANCE

A continuación se describe a detalle los objetivos que tiene el centro de cómputo integrado en las instalaciones de El Independiente de Hidalgo.

#### OBJETIVO GENERAL

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

#### OBJETIVOS ESPECIFICOS

Se tiene con objetivos específicos los cuales nos indican a detalle lo que se pretende lograr, para ello se lleva un control (bitácora). Los objetivos del Independiente de hidalgo en su centro de cómputo se enlistan a continuación:

* Verificación del sistema eléctrico de la sala de informática.
* Verificación de la comunicación interna y externa en red LAN
* 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.

### 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.

### 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.
* Requerimientos de Usuarios

### ORGANIGRAMA

### 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.

* **Edgar Toledo Robles:** Jefe de área de Sistemas.
* **Susana Lopez Galván:** Encargada de sistemas en área de redacción.
* **Solibeth González:** Corrector.
* **Emilio Gutiérrez Ayala:** Paginador.

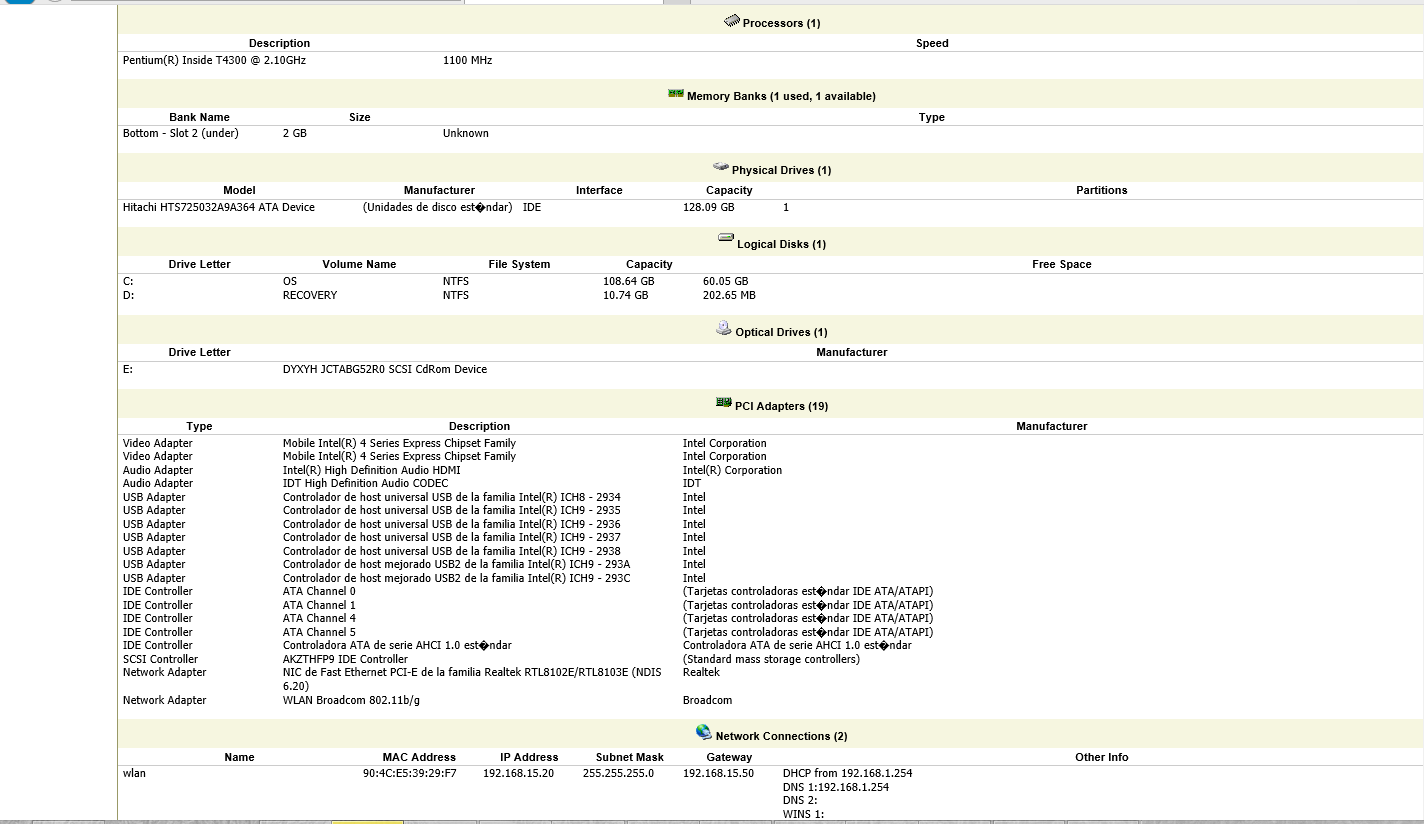
### TIPO DE SOFTWARE A UTILIZAR

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

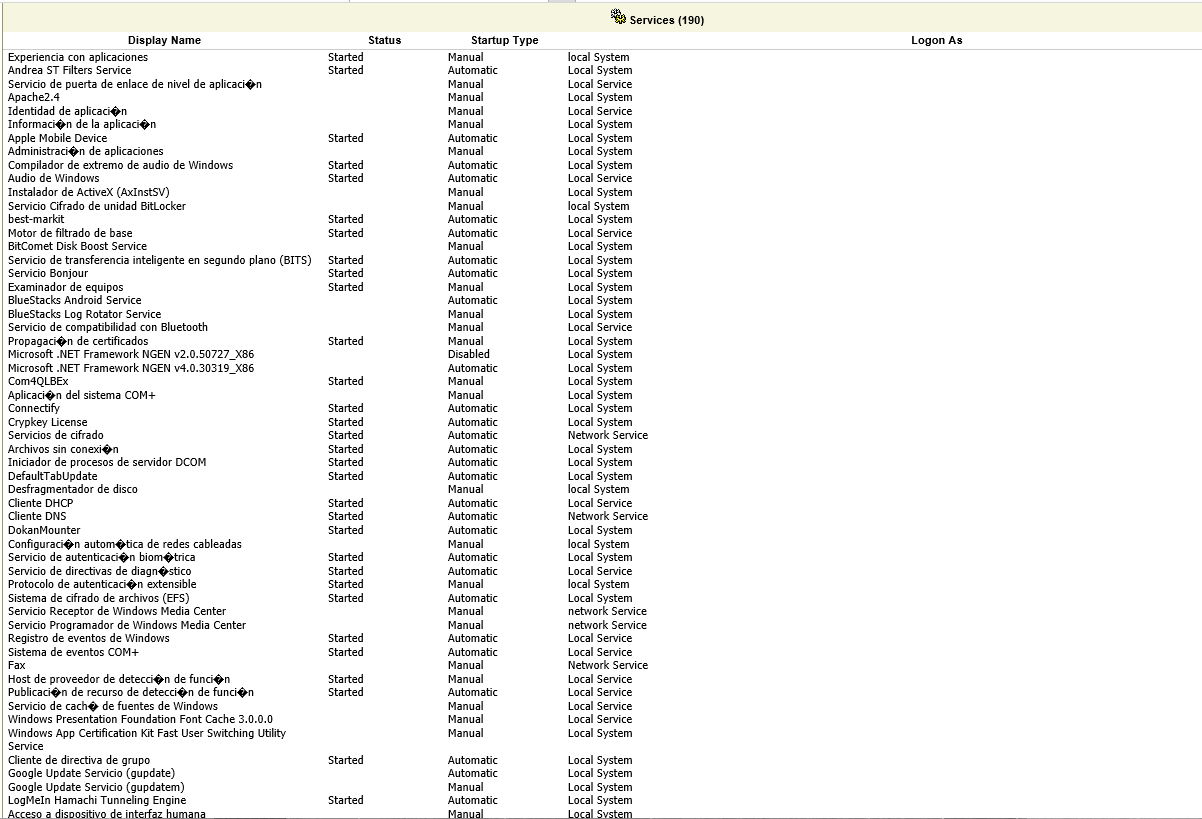
#### CERTERO PCAUDITOR

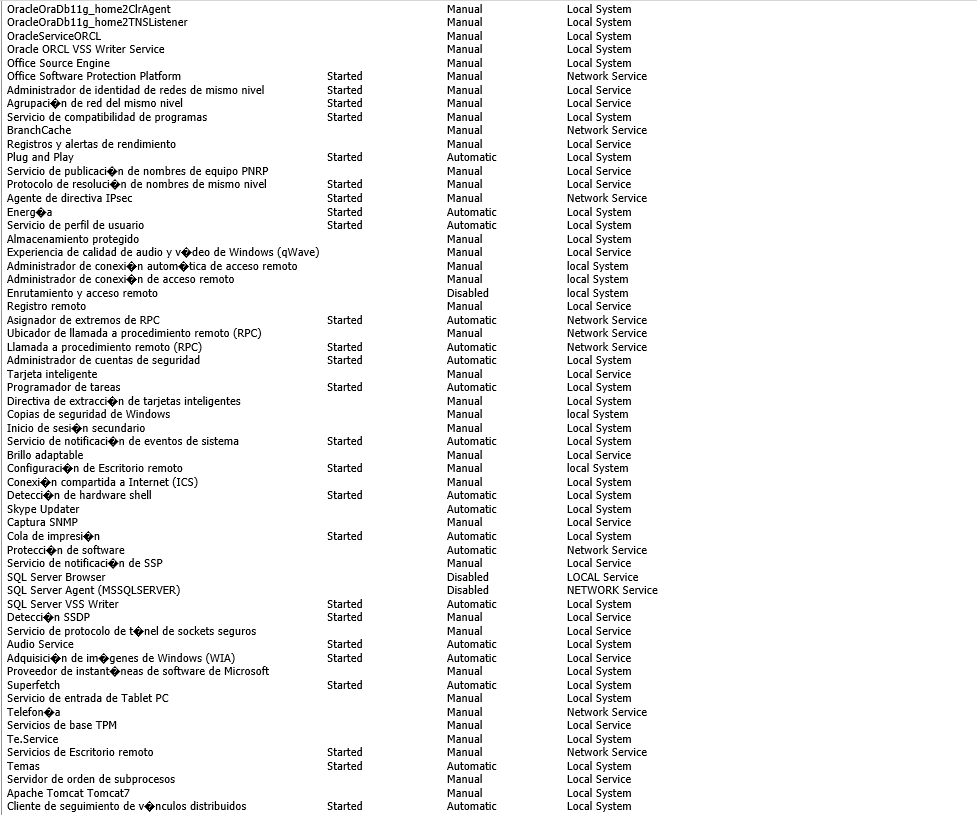
Tras haberse sometido las computadoras con Microsoft Windows Vista a una auditoría utilizando el software *Certero PC Auditor* para ello, los resultados fueron los siguientes:

**Hardware**

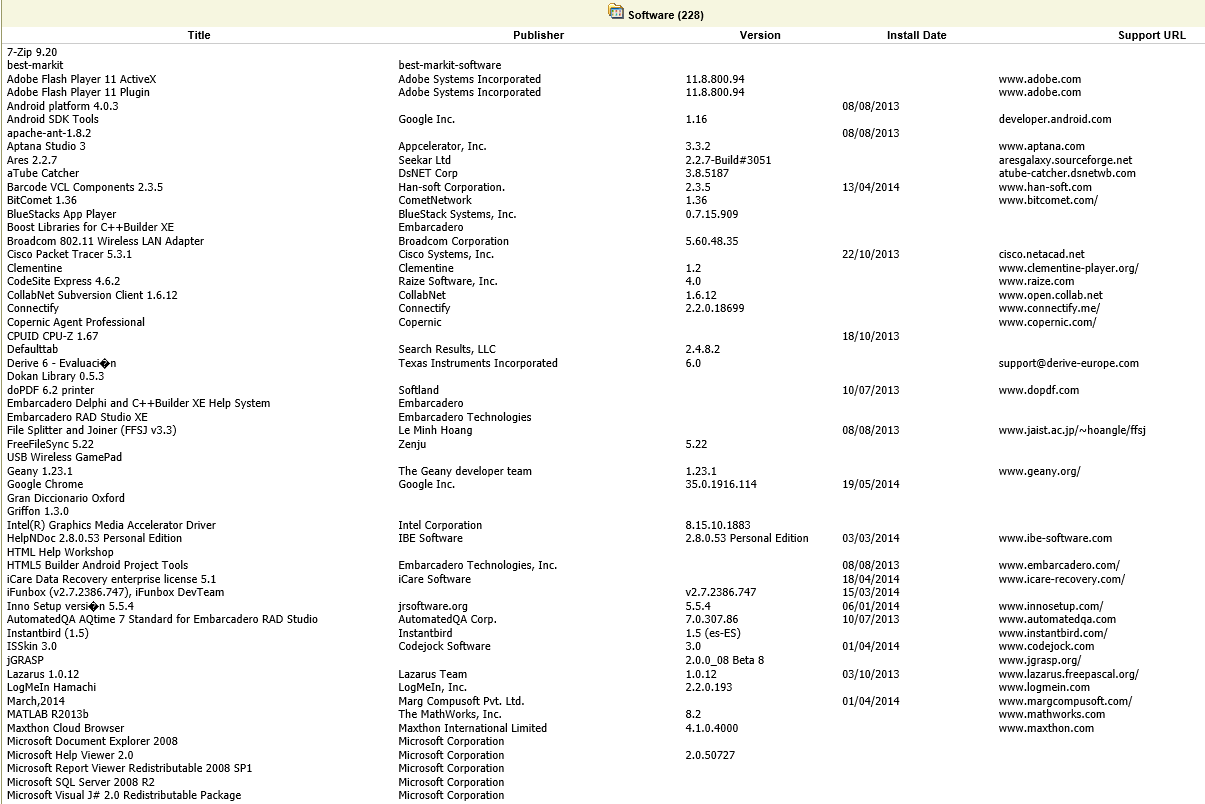


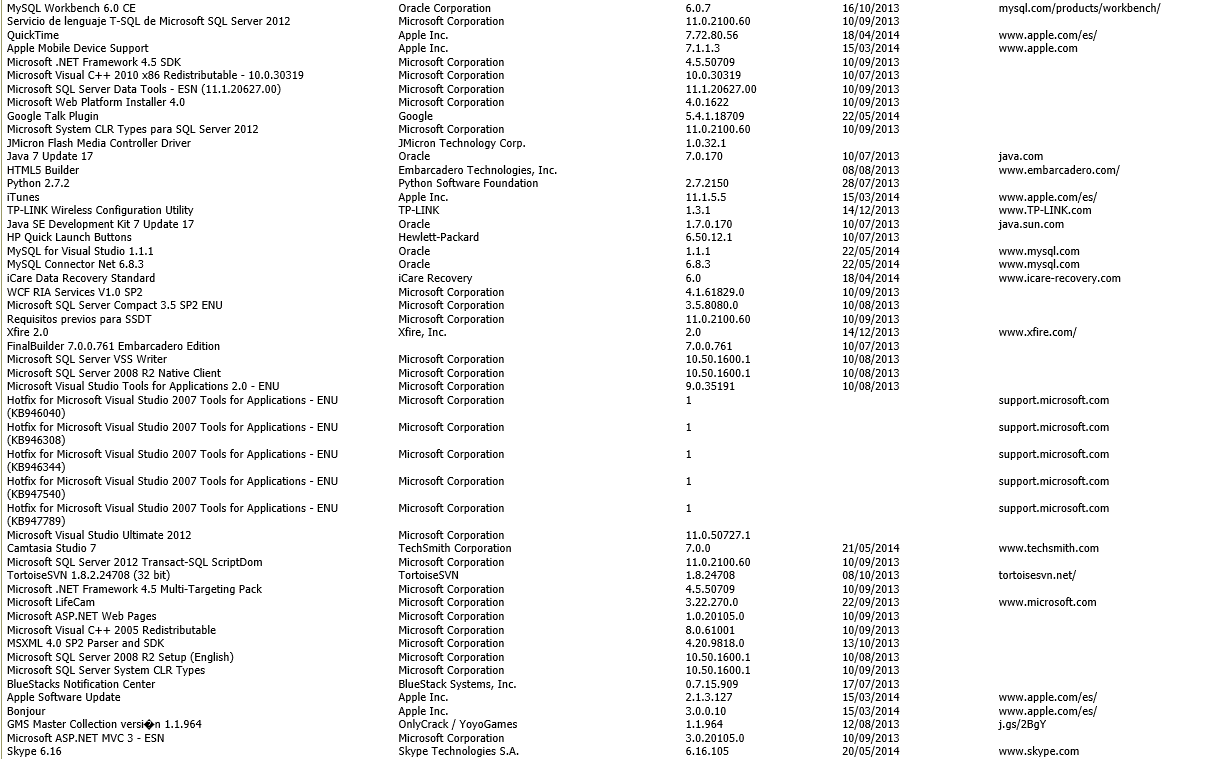
**SERVICES**



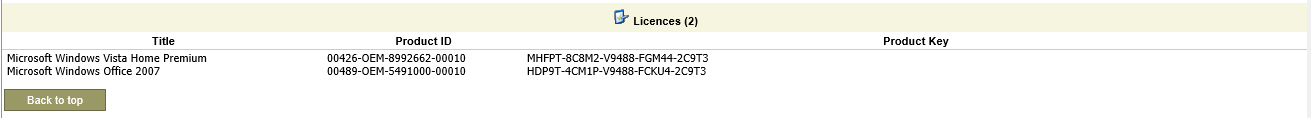


**SOFTWARE**

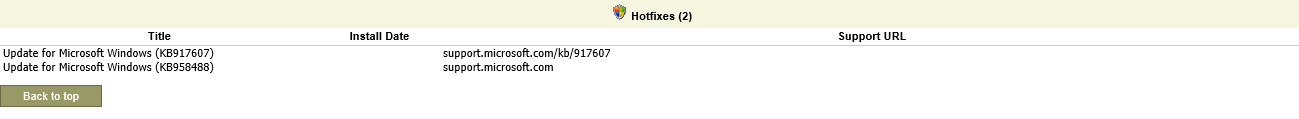




**LICENCES**



**SOPORTES**



## 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 responde a lo siguiente:**

* ¿Las condiciones de las salas de informática están acorde a las normas de seguridad industrial establecidas? No del todo.
* ¿Los equipos de cómputo se encuentran en las condiciones mínimas requeridas para la prestación del servicio? Si.
* ¿Las redes alámbricas e inalámbricas se encuentran protegidas con contraseña, para evitar la intromisión de personal ajeno a la institución? Si.
* ¿La ofimática de la sala se encuentra debidamente legalizada? Si.
* ¿Las personas a cargo del mantenimiento de las salas, son idóneas y están capacitadas para dar respuesta oportuna a las necesidades de la misma? Si.
* ¿Actualmente se encuentra con una diagramación de red a prueba de fallos? Está en proceso.

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

### 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.

### 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” marca HP
* **Mouse:** Mouse alámbrico
* **Teclado:** Teclado Acteck alámbrico
* **Ups:** UPS Liebert Gxt6000t- 240xa.
* **Reguladores de Voltaje:** Complet 1300va 8 contactos

## PUNTOS DEBILES Y AMENAZAS.

### MATRIZ FODA(PROPUESTA)

|  |  |
| --- | --- |
| **Factores internos**  **Controlables** | **Factores externos**  **No controlables** |
| **Fortalezas**  **(+)**   * Personal egresado de la U.A.E.H. * Personal comprometido a mejorar y entregar lo mejor de sí. * Equipo de cómputo mantenido al día. * Ambiente laboral agradable. * Producto en constante renovación. | **Oportunidades**  **(+)**   * Expansión de mercado al mercado móvil. * Difusión por parte de Radio Universidad. * Aplicación de suscriptores para iOS y Android. |
| **Debilidades**  **(-)**   * Mantenimiento nulo a equipos de servidores. * Mantenimiento nulo a estaciones de trabajo. * Ubicación del SITE poco favorable. | **Amenazas**  **(!)**   * Falta de ventilación en las oficinas de edición y en la de reporteros; esto puede provocar sobrecalentamiento. * El UPS del diario no soporta la cantidad de equipos de cómputo, por ende tiende a soportar unos cuantos minutos manteniendo las oficinas con energía eléctrica. * Falta de hidrantes en las demás oficinas en caso de incendio. |

### 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:

* Ubicar los equipos de tal forma que no presenten un riesgo, tanto para el alumno como para la misma entidad.
* 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.

## 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.

### 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:

* En caso de que exista algún daño, será difícil determinar 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.

### RECOMENDACIONES

A partir de lo observado en los puntos débiles y amenazas y con base en la norma y en un plazo no muy largo, dar solucionar de fondo que garanticen la correcta colocación del SITE.

## 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.

### 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.

### 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.

## CONEXIONES DE REDES

Al hablar de las conexiones de redes que utilizan en el centro de cómputo del Independiente, es posible determinar que el tipo de red que se utiliza es una red de área local estrella, ya que existen dos *switches* cuyo único fin es el de distribuir la conexión y conectar las estaciones de trabajo.

### Puntos débiles y amenazas

* Al tener *switches*, la banda ancha se distribuye, por ende, la velocidad total de esta es dividida entre el número total de elementos conectados al switch.

## 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.

### PUNTOS DÉBILES Y AMENAZAS

Existen algunas deficiencias en cuanto a las licencias, ya que solamente se encontraron muy pocos programas con licencia válida, en cuanto al resto de los programas instalados en las máquinas del centro de cómputo, no tienen licencia o son software libre.

### RECOMENDACIONES

Se recomienda ampliamente utilizar software con licencia libre para evitar posibles problemas a futuro.

### PLANES DE CONTINGENCIA

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

## 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.

### 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.

## Bases de datos, propietarios de la información y usuarios de la misma.

El Independiente de Hidalgo cuenta con un par de base de datos: “desarrollo” e “independiente”; cada una constando de 207 tablas, 35 vistas, 8 funciones y 1 evento. La primera base de datos es una réplica de la estructura de la segunda.

La diferencia radica en que la base de datos llamada “desarrollo” es utilizada para fines de práctica, desarrollo y pruebas, mientras que la llamada “independiente” contiene datos de producción; datos como nombres de suscriptores reales, rutas reales, etcétera.

### Propietarios de la información

En el periódico no existe como tal un propietario de la información almacenada dentro de las bases de datos, sin embargo, el administrador de la base de datos es el jefe del área de sistemas (L.S.C. Edgar Calderón Toledo).

### Usuarios de la base de datos

Los usuarios que acceden a la base de datos e insertan nuevos datos son 34; periodistas, agentes de ventas, administradores, recepcionistas, responsables de publicidad y circulación, contadores, y el propio administrador de los sistemas y administrador de bases de datos.

Los usuarios que acceden a esta, tienen permisos y niveles. Gracias a estos últimos, cierto grupo de usuarios pueden realizar tareas que a su área corresponde, y, ciertamente, no pueden saber lo que sucede con los demás usuarios ni los procesos que estos llevan a cabo.

## Procedimientos y políticas en caso de desastre

Es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que El Independiente de Hidalgo pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

A continuación se presenta la propuesta de procedimientos y políticas y procedimientos para en caso de desastres para aplicar en El Independiente de Hidalgo

### OBJETIVOS GENERALES Y ESPECÍFICOS

#### Generales:

Garantizar la continuidad de las actividades del EL INDEPENDIENTE DE HIDALGO, ante eventos que podrían alterar el normal funcionamiento de la Tecnología de la Información y Comunicaciones - TICs, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales.

#### Específicos:

* Contar con documentación práctica y actualizada que garantice al EL INDEPENDIENTE DE HIDALGO la continuidad de las operaciones de los sistemas informáticos sin sufrir paralizaciones o pérdidas relevantes.
* Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.
* Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que ésta no exceda las 24 horas.
* Contar con personal debidamente capacitada y organizada para afrontar adecuadamente las contingencias que puedan presentarse en las actividades del EL INDEPENDIENTE DE HIDALGO.

### ALCANCE

La Implementación del Plan de Contingencia informático, incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la institución.

### Acciones a ser consideradas:

* **Antes**, como un plan de respaldo o de prevención para mitigar los incidentes.
* **Durante**, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
* **Después**, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

El Plan de Contingencia permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

El término “incidente” en este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático en el EL INDEPENDIENTE DE HIDALGO.

### Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

### Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

Plan de Recuperación Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Todo Plan de Contingencia informático debe tener un carácter recursivo que permita retroalimentar y mejorar continuamente los planes en cada una de las etapas descritas, logrando así tener un documento dinámico.

### Plan de Pruebas

El Plan de Pruebas, será presentado a la Dirección Ejecutiva del EL INDEPENDIENTE DE HIDALGO para su aprobación previa a su implementación. El resultado de las pruebas efectuadas será presentado igualmente para su conformidad.

Las pruebas relacionadas a este plan, se ejecutaría semestralmente, mes de Junio y Diciembre con el fin de evaluar la preparación de la organización ante la ocurrencia de un siniestro y realizar los ajustes necesarios.

### METODOLOGÍA

La presente metodología es el resultado de la experiencia práctica de EL INDEPENDIENTE DE HIDALGO en la implementación de planes de contingencia, mitigación de riesgos y seguridad, también en base a experiencias en otras instituciones, lo cual garantiza que el documento final sea necesariamente objetivo y práctico, a fin de contar con una herramienta efectiva en caso de una contingencia real.

Para elaborar el Plan de Contingencia se seguirá una metodología que tiene las siguientes fases:

* Fase 1: Organización
* Fase 2: Identificación y priorización de riesgos
* Fase 3: Definición de eventos susceptibles de contingencia
* Fase 4: Elaboración del Plan de Contingencia 6
* Fase 5: Definición y Ejecución del Plan de Pruebas
* Fase 6: Implementación del Plan de Contingencia

Fases de la metodología propuesta:

### Organización del Plan de Contingencia

Uno de los aspectos que evidencia un carácter formal y serio en toda organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la organización en el Plan de Prevención, Ejecución y Recuperación, pero definiendo un grupo responsable para su elaboración, validación y mantenimiento.

### Identificación y Priorización de Riesgos

Denominamos INCIDENCIA al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

### Elaboración de los Planes de Contingencia

Una de las fases importantes del Plan de Contingencia es la documentación y revisión de la información que se plasmará en una guía práctica y de claro entendimiento por el personal del EL INDEPENDIENTE DE HIDALGO.

Es por ello, que una fase importante de la metodología considera un formato estándar de registro de todos los eventos definidos que forman parte del plan, así se tendrá finalmente un entregable acorde con los requerimientos y políticas definidas para tal fin.

### Definición y ejecución del plan de pruebas

Conscientes que una situación de contingencia extrema puede presentarse en cualquier momento, y por ende convertirse en un problema prioritario de atender si éste se produjera en el horario de oficina que pueda resultar impactante durante las actividades del EL INDEPENDIENTE DE HIDALGO; es que se hace necesario definir de manera específica todas las acciones necesarias para asegurar que, en caso real de contingencia y tener un conjunto de prestaciones y funcionalidades mínimas que permitan posteriormente ejecutar el plan de recuperación de manera rápida y segura

### Implementación del Plan de Contingencia

La implementación del presente plan se realizará en el segundo mes de su aprobación.

### DESARROLLO DE LAS FASES, ACTIVIDADES, ESTRATÉGIAS, PROGRAMAS Y POLÍTICAS

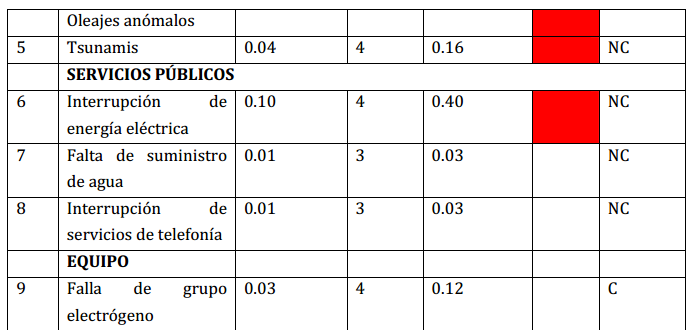
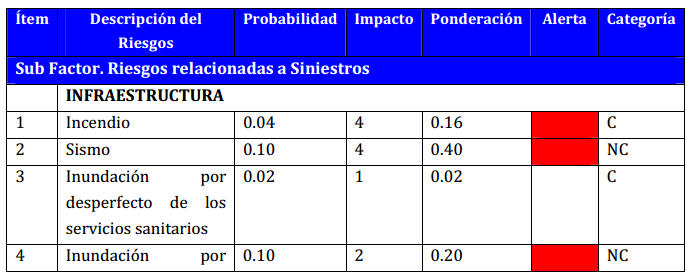
Como parte del presente capítulo, la Unidad de Informática, plantea el desarrollo de los tópicos, utilizando la metodología expuesta anteriormente. Este desarrollo incluirá las siguientes fases de la metodología

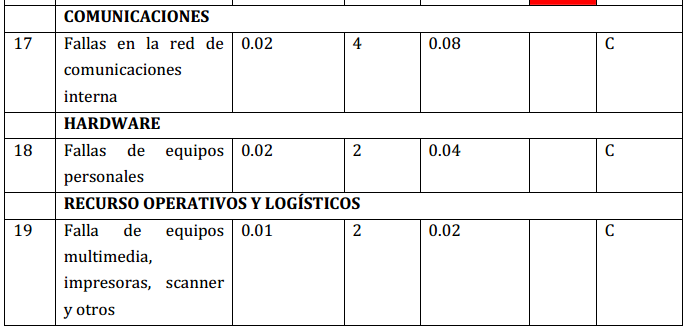
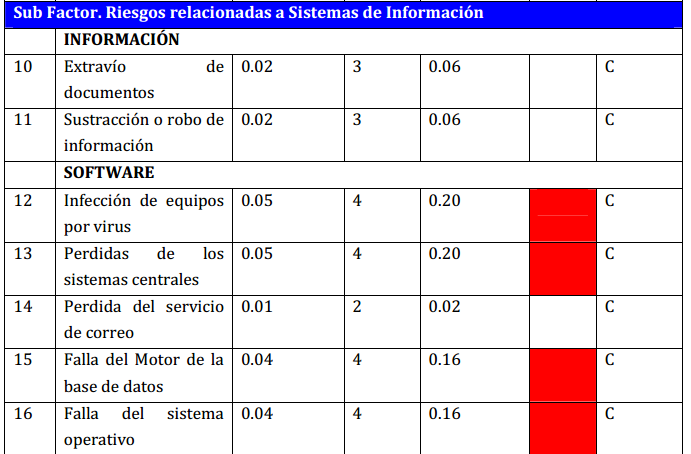
* Identificación y Priorización de riesgos
* Definición de Eventos susceptibles de Contingencia.
* Elaboración del Plan de Contingencia.

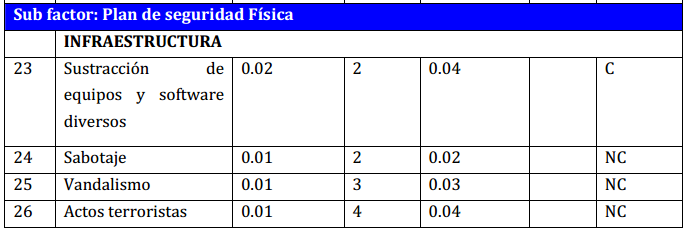
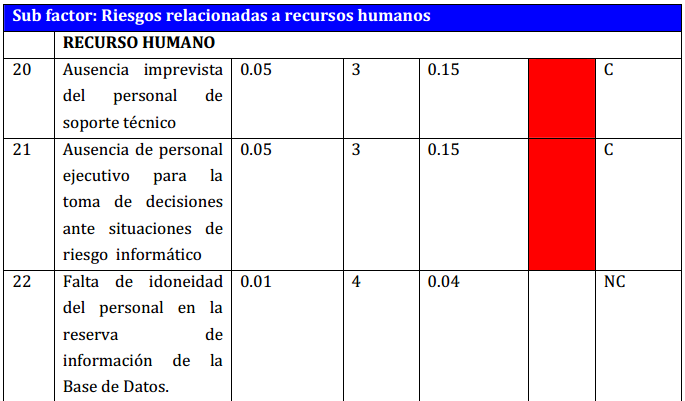
### Identificación y Priorización de Riesgos

El cuadro N °4 muestra la matriz de Riesgo de Contingencia, ponderado de acuerdo a los valores de riesgo e impacto en el servicio (operatividad), usando el conocimiento y la experiencia práctica de Informática en Gestión de Sistemas de Información:

Cuadro N °4: Matriz de Riesgo de Contingencia





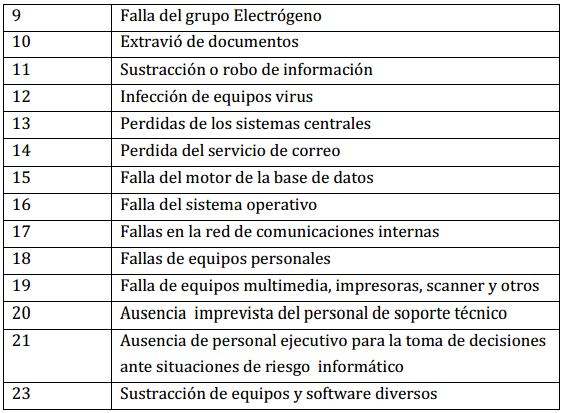
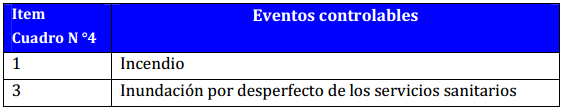


Nota: El color rojo de la alerta representa que el evento es altamente impactante en el servicio por lo tanto debe ser obligatoriamente controlado.

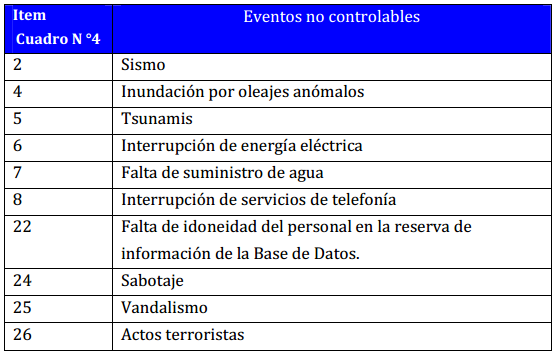
En la columna CATEGORÍA por cada evento, se considera la identificación de aquellos eventos Controlables (C), y No Controlables (NC).

En los cuadros N° 5 y N° 6 se resumen los eventos según la categorización de eventos controlables y no controlables:

Cuadro N °5: Eventos Controlables



Cuadro N °6: Eventos no Controlables



Hackeo

## Sistemas propios y/o legalidad de los mismos.

El jefe de sistemas del diario “El Independiente de Hidalgo” ha desarrollado las aplicaciones que se utilizan a diario en El Independiente, tales como la aplicación que utiliza el jefe de Circulación, un módulo para enviar facturas a los suscriptores, un sistema tarificador para clasificar y obtener informes sobre las llamadas registradas diariamente por el conmutador del diario, la aplicación “Independiente”, que contiene todos los módulos de la empresa, entre otras, tales como la aplicación móvil para quienes reparten periódico por las mañanas.

En cuanto a software dentro del diario, cada computadora cuenta con el sistema operativo Microsoft Windows Vista con licencia, navegadores libres como Mozilla Firefox y Google Chrome.

Asimismo, El software con licencia con el que cada equipo de cómputo cuenta son los siguientes:

* Adobe Creative Suite 6.
* Microsoft Office 2010.

### Pruebas Sustantivas

Las pruebas que reciben esta denominación son aquellas que un auditor, en su calidad de asesor, plantea, con la finalidad de obtener convicción o evidencia clara, concisa y precisa referente a la información financiera observada. Éstas tienen relación directa con principios como la imparcialidad y objetividad; además están orientadas a ser base que sustente la validez y confiabilidad de la información analizada.

|  |  |
| --- | --- |
| Pruebas para identificar vulnerabilidades en el servidor. | 1. Permitir a un atacante acceder a información confidencial. 2. Permitir a un atacante modificar información 3. Permitir a un atacante negar un servicio. |
| Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad. | Las pruebas se pueden realizar suministrando información al responsable (por ejemplo direcciones IP) de su ejecución o se pueden realizar también sin suministrar esta información. También estas pruebas se pueden clasificar según si se hacen en la red interna o se intentan ataques desde fuera de la red, es decir, intentar llegar a la red interna desde por ejemplo Internet, pasando por el firewall o algún otro dispositivo de frontera.   1. Internas    1. Sin conocimiento    2. Con conocimiento 2. Externas    1. Sin conocimiento    2. Con conocimiento |
| Pruebas para asegura la calidad de los datos. | 1. Estimar y planificar la cantidad y tipo de pruebas previas a implementar durante el desarrollo de ésta (incluyendo el o los objetivos generales y específicos de cada una de ellas, y en especial las decisiones a adoptar a partir de los resultados alcanzados) con el fin de incrementar la calidad de los datos. |
| Pruebas para identificar la inconsistencia de los datos. | 1. establecer las actividades de supervisión y monitoreo durante el trabajo de campo; |
| Pruebas para comparar con los datos o contadores físicos. | Considerar la metodología de evaluación de cobertura y de contenido a implementar, una vez que se cuente con los datos relevados hasta alcanzar su difusión total y definitiva. |
| Pruebas para determinar y/o remplazar el equipo de cómputo actual. | * + - 1. Realizar pruebas de performance. |
| Pruebas para identificar el uso inadecuado del equipo. | 1. Identificar el uso de la conexión a internet. 2. Identificar el software instalado. 3. Restringir el acceso a redes sociales y software de ocio. |

### INFORME DE AUDITORIA

**INFORME DE AUDITORIA**

**1. Identificación del informe**

Auditoria física.

**2. Identificación del Cliente**

Departamento De Sistema, área de redacción.

**3. Identificación de la Entidad Auditada**

“El Independiente de Hidalgo”.

**4. Objetivos**

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

**5. Hallazgos Potenciales**

* No existe un calendario de mantenimiento
* Falta de ventilación.

**6. Alcance de la auditoria**

* La presente auditoría abarca el periodo el periodo escolar enero-diciembre de 2014 y ha sido realizada en El Independiente de Hidalgo, en específico al área de sistemas y redacción de la institución.
* 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. 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.

**8. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | PLANEAMIENTO | EJECUCIÓN | INFORME |
| FECHAS | **01 De Enero al 30 Mayo** | **1 DE Marzo AL 1 DE Mayo** | **20 DE MAYO** |

**9. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| APELLIDOS NOMBRES | CARGOS |
| Jonathan Salas Hernández | **Auditor Líder** |
| David Zahid Jiménez Grez | **Auditor junior** |
| Adalberto Vargas Moreno | **Auditor junior** |
| Christian Yamil Castillo Covarrubsd | **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 de 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**

**BALANCE DE RESULTADOS**

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

**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) |

### INFORME DE AUDITORIA

**1. Identificación del informe**

Informe de la auditoría.

**2. Identificación del Cliente**

Es del sector privado.

**3. Identificación de la Entidad Auditada**

Empresa de capital privado, sociedad anónima de capital variable.

**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.

**8. Recomendaciones**

* Se recomienda contar con sellos y firmas digitales.
* Creación de 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.

**9. Fecha Del Informe**

**PLANEAMIENTO EJECUCION INFORME**

|  |  |  |  |
| --- | --- | --- | --- |
|  | PLANEAMIENTO | EJECUCIÓN | INFORME |
| FECHAS | **01 De Enero al 30 Mayo** | **1 DE Marzo AL 1 DE Mayo** | **22 DE MAYO** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| APELLIDOS NOMBRES | CARGOS |
| Jonathan Salas Hernández | **Auditor Líder** |
| David Zahid Jiménez Grez | **Auditor junior** |
| Adalberto Vargas Moreno | **Auditor junior** |
| Christian Yamil Castillo Covarrubias | **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:

* Normativa a cumplir
* 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

**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**

“El Independiente de Hidalgo”.

**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:**

Gracias a los resultados obtenidos, se puede concluir que la evaluación de cada uno de los objetivos contenidos en el programa de auditoría informática se ha cumplido.

El área de informática presenta algunas observaciones, 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 Enero al 30 Mayo** | **1 DE Marzo AL 1 DE Mayo** | **22 DE MAYO** |

**10. Identificación Y Firma Del Auditor**

|  |  |
| --- | --- |
| APELLIDOS NOMBRES | CARGOS |
| Jonathan Salas Hernández | **Auditor Líder** |
| David Zahid Jiménez Grez | **Auditor junior** |
| Adalberto Vargas Moreno | **Auditor junior** |
| Christian Yamil Castillo Covarrubias | **Auditor junior** |

**BALANCE DE RESULTADOS**

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

# CONCLUSIONES

Con base en lo mostrado anteriormente se concluye 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% 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.

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 Independiente de Hidalgo cuenta con la siguiente información:

* Planes de seguridad y continuidad
* Contratos, pólizas de seguros.
* Organigrama y manual de funciones.
* Requerimientos de Usuarios
* Políticas, estándares, normas y procedimientos.

Sin embargo, carece de lo siguiente:

* Plan de sistemas.
* Manuales de sistemas.

De la información que se carece, se elaborará e implementará de la siguiente manera:

|  |  |  |  |
| --- | --- | --- | --- |
| TIPO DE DOCUMENTO | RESPONSABLE | FECHA ESTIMADA ELABORACION | FECHA ESTIMADA DE IMPLEMENTACIÓN |
| MANUALES DE SISTEMAS. | L.S.C EDGAR CALDERÓN TOLEDO | 3 MESES | 6 MESES |
| PLAN DE SISTEMAS. | L.S.C EDGAR CALDERÓN TOLEDO | 6 MESES | 1. AÑO |

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. Con ello, se confirma el compromiso y la oportunidad de avanzar hacia la mejora continua en la organización.

# 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) |

# AREAS DE OPORTUNIDAD O DE MEJORA

Con fundamento en lo mostrado anteriormente se tiene que El Independiente de Hidalgo puede mejorar si el director del área de informática; que actualmente es el Lic. Edgar Toledo, documenta debidamente lo siguiente:

* Plan de contingencia.
* Plan de redes.
* Plan de ofimática.

Adicionalmente para El Independiente de Hidalgo, son desconocidos los criterios para el análisis y medición y seguimiento de los resultados de operación de procesos, puesto que no se encuentra evidencia documental de que se realice la evaluación de la realización de productos, ni la evaluación de su desempeño, la sugerencia es documentar dicha evidencia, por parte de Lic. Edgar Toledo, director del área de sistemas.

Según las observaciones echar por parte del equipo de trabajo auditor, el personal de El Independiente de Hidalgo mostró interés en trabajar utilizando las normas que regulan a los planes respectivos.