# UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

ESCUELA DE CONTABILIDAD Y ADMINISTRACION


**Desarrollo de una Guía Práctica para la Aplicación de Auditorías en Informática**

TESIS

**Que para obtener el Título de:**

LICENCIADO EN INFORMATICA

**PRESENTAN:**

**MONTIEL HERRERA NOEMI**
**ESTRADA SANCHEZ RAMONA**
**SANCHEZ ESPINOZA SONIA RAQUEL**

**ENSENADA, B. C.** **AGOSTO DE 1997**

# UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

## ESCUELA DE CONTABILIDAD Y ADMINISTRACIÓN


# DESARROLLO DE UNA GUÍA PRÁCTICA PARA LA APLICACIÓN DE AUDITORÍAS EN INFORMÁTICA

QUE PARA OBTENER EL TÍTULO DE:
LICENCIADO EN INFORMÁTICA

PRESENTAN
MONTIEL HERRERA NOEMÍ
ESTRADA SÁNCHEZ RAMONA
SÁNCHEZ ESPINOZA SONIA RAQUEL

APROBADO POR:

M.A.I. OMAR ÁLVAREZ XOCHIHUA

ENSENADA, BAJA CALIFORNIA AGOSTO DE 1997.

# UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

## ESCUELA DE CONTABILIDAD Y ADMINISTRACIÓN

# DESARROLLO DE UNA GUÍA PRÁCTICA PARA LA APLICACIÓN DE AUDITORÍAS EN INFORMÁTICA

**TESIS**

**QUE PARA OBTENER EL TÍTULO DE:**

## LICENCIADO EN INFORMÁTICA

**PRESENTAN :**

**MONTIEL HERRERA NOEMÍ**
**ESTRADA SÁNCHEZ RAMONA**
**SÁNCHEZ ESPINOZA SONIA RAQUEL**

**ENSENADA, BAJA CALIFORNIA** **AGOSTO DE 1997.**

# DEDICATORIAS

A Dios:

Por permitirme lograr una de las metas más importantes de mi camino.

A mi Madre:

Por darme tanto y tanto amor, por hacerme sentir muy importante en su vida, por ser la inspiración de muchas de mis acciones en el camino y por ser el motivo de mi vida.

A mi hermano Manuel:

Por todos sus esfuerzos, por sacar adelante a mí y a mis hermanos, por ser siempre conmigo una gran persona.

A mi hermana Lili:

Por ser siempre mi mejor amiga, mi mejor hermana y en muchas ocasiones una gran Madre, por motivarme y darme la voluntad de hacer las cosas, por todos sus sacrificios y cansancio, por su tiempo dedicado a mi superación como persona y profesionista.

A mi hermana Teresita:

Por ser siempre una gran hermana, por apoyarme e impulsarme en todo lo que hago, por demostrarme siempre su cariño.

A mi hermana Oly:

Por ser la persona que le dio tantos matices a mi infancia y adolescencia y por ser tan alegre y singular.

A mi hermano Obet:

Por ser un ejemplo de lo que se quiere se puede lograr, por motivarme a superarme, por todo su cariño y por tratar siempre de transmitirme su fuerza.

A mi hermana Sandra:

Por ser para mí, un ejemplo de superación, por ser mi mejor amiga, por ser una gran compañera de vida, por tratar siempre de impulsarme y transmitirme seguridad en mí.

A mis sobrinos:

A esos diez enanos que han llegado a cambiarnos la vida y darnos tantos y tantos motivos para vivir y ser felices.

A mis cuñados y cuñadas: MEMO, GUERA, MARY Y LUIS:

Por apoyarme siempre y aguantar a mis respectivos hermanas y hermanos.

Noemí Montiel Herrera.

A mi gran Dios por hacerme sentir su hija en todos los momentos de mi vida.

A mis Padres por su ejemplo y amor, pero muy especialmente a mi Madre por su tiempo, por su entrega total, por ese espíritu de lucha, por esos días de desvelo al iniciar y terminar mi carrera, Gracias Mami.

A mi amado esposo por su GRAN apoyo y comprensión, por ser siempre la persona que me motiva en los momentos difíciles de mi vida, por compartir con alegría su vida con la mía: Gracias por Amarme.

A mis hermanas Fidelia, Marytere y Marysol, por su cariño y motivación hacia mi persona.

Ramona Estrada Sánchez

# AGRADECIMIENTOS

A mi AMIGA Mónica:

Por saber ser una verdadera compañera de trabajo y por ser mucho mejor amiga.

A M.A.I. Omar Alvarez:

Por haber tenido la grata oportunidad de conocerlo, de haber recibido una valiosa colaboración en el desarrollo de esta tesis, y por brindarnos tanta paciencia, PROFESIONALISMO, y gran calidad humana.

A mi Escuela:

Alma Mater: Por haberme brindado la oportunidad de lograr el objetivo de culminar una carrera Universitaria.

A mis Maestros:

Por recibir una parte de su conocimiento, por sus opiniones y consejos: Muchas Gracias.

Noemí Montiel Herrera.

Deseo expresar mi más sincero agradecimiento al M.A.I. Omar Álvarez Xochihua, por el gran apoyo que nos brindó para la realización de esta tesis.

Agradecerle también de manera muy especial a mi Jefe, el Sr.Sergio Tejeda por toda su paciencia, comprensión y apoyo.

Así mismo al Lic. Alfonso Talavera por todas las facilidades prestadas y el apoyo brindado para la realización exitosa de esta tesis.

A Noemí por toda su paciencia y entrega, gracias por ser mi Amiga.

A todos mis maestros, gracias por sus conocimientos, pero sobre todo gracias porque de cada uno me llevo algo valioso para mi diario caminar.

A todos aquellos que de alguna manera contribuyeron a la elaboración de esta tesis.

Ramona Estrada Sánchez

Para quienes me acompañaron en mi vida y hoy ya no están conmigo, y para quienes hoy forman parte de mi presente y mi futuro...

Sonia Raquel

# ÍNDICE

## LISTA DE TABLAS

## LISTA DE FIGURAS

# CAPÍTULO I
# INTRODUCCIÓN

"Actualmente, las Organizaciones han cambiado dinámica y significativamente la forma de hacer las cosas (desde un enfoque operativo), esto es, de procesos cien por cien manuales y primitivos, se ha llegado a la automatización; y un número cada vez mayor de empresas está automatizando sus actividades básicas.

Ahora se busca tener una empresa con la información en línea; en otras palabras, brindar a la dirección todos los datos necesarios de cualquier proceso en el momento y forma adecuada para la toma de decisiones.

La manera de planear y administrar las estrategias y tácticas de la empresa dejó de ser un proceso lento, complejo y de un puñado de ejecutivos, convirtiéndose en un proceso administrable, dinámico, proactivo y visionario, a través del apoyo de metodologías Organizacionales y herramientas productivas de tecnología informática." [1]

Todo lo anterior, es una realidad palpable en cuanto al avance y transformación que con el paso del tiempo y la evolución tecnológica de hoy en día, han logrado las empresas. Pero no ha sido tan fácil ni mágico, se han enfrentado a diferentes situaciones que han resuelto para lograr la eficiencia y productividad requerida para que una organización funcione correctamente.

Actualmente se requiere de sistemas de información más precisos, confiables y oportunos tanto en el sector público como en el privado, por lo que es necesario considerar a la Informática de gran relevancia en las actividades Organizacionales. Los sistemas de información automatizados, han sido y son de gran ayuda para las Organizaciones que manejan volúmenes grandes de información, ya que con ellos eficientizan el proceso de la misma.

[1] Hernández Hernández Enrique . Auditoría en Informática. 1995.

En el terreno de los sistemas de información, un alto porcentaje de las empresas tienen problemas en el manejo y control, tanto de los datos como de los dispositivos en que almacenan, procesan y distribuyen la información. Esta situación genera tiempos de respuesta inadecuados en la recopilación, proceso y entrega de los resultados, así mismo, origina incertidumbre acerca de la productividad de los recursos involucrados en las operaciones diarias.

Cabe mencionar que muchas empresas no están dispuestas a invertir dinero y tiempo para eliminar problemas, como la falta de conocimiento del alcance de sus sistemas de información, la capacitación inadecuada del personal de informática, la planeación y desarrollo inadecuado para la administración de sus funciones, entre otros.

El principal error al que se enfrentan estas Organizaciones, es no realizar un análisis previo para resolver sus necesidades de equipo de cómputo , software, personal, e información, ocasionando por lo general, un descontrol en donde es requerida la aplicación inmediata de una Auditoría en Informática.

Si actualmente la alta gerencia toma decisiones estratégicas, basadas en informes provenientes de sistemas electrónicos, entonces es indispensable aumentar la eficacia y reducir el riesgo de error con la utilización de técnicas y controles que dén seguridad a la información.

Esto lo podemos solucionar a través de la Auditoría en Informática, ya que es la encargada de la revisión sistemática y evaluación permanente de los controles, sistemas, procedimientos de Informática, equipo de cómputo, su utilización, eficiencia y seguridad dentro de la Organización, con la finalidad de determinar el grado de eficiencia con que ésta opera, constituyendo una búsqueda para localizar los problemas en el funcionamiento de la misma, así como sus aciertos.

La Auditoría en Informática debe ser realizada por personal que tenga amplio conocimiento en el área, auxiliado por otros profesionistas como los Contadores Públicos y Administradores, con apego a las normas que el código de ética de los Auditores en Informática señala.

Hablando en forma práctica, la Auditoría en Informática es una labor que se debe tomar con seriedad y profesionalismo, ya que los resultados que ésta arroje, servirán a la Gerencia o Dirección de la Organización en la toma de decisiones sobre el cuidado de sus recursos de información.

Existen muchas formas de realizar Auditorías en Informática, ya que esto depende de muchos factores como lo son el giro de la empresa, el tamaño, el equipo con que trabaja, el personal que labora entre muchos otros, así que llevarla a cabo es una tarea muy seria y laboriosa; todas y cada una de las actividades que requiere una Auditoría son importantes, pero una de las más importantes, es la elección de una metodología, ya que la función de Auditoría en Informática, desarrolla sus actividades basándose en un método de trabajo formal que sea entendido por todos los auditores en informática.

La idea principal de este trabajo, es el desarrollo de una guía práctica para la aplicación de Auditorías en Informática, con la cual, se pretende apoyar y brindar a los Auditores en Informática y profesionistas en el área de cómputo, un elemento metodológico para cubrir satisfactoriamente los temas de Auditoría, seguridad y control inherentes a la función de informática en cada una de sus áreas. La guía contará con ejemplos, cuestionarios, formatos prácticos para la recopilación de información que facilitarán al Auditor, la realización de las tareas y actividades propias de una Auditoría en Informática dentro de un proceso metodológico.

Esta guía práctica, es resultado de las investigaciones realizadas por la necesidad de elegir una metodología para aplicar una Auditoría en Informática.

Para tener una visión real de la utilidad de la guía que desarrollamos, se pondrá a prueba a través de un caso práctico, el cual consistirá en Auditar el centro de cómputo de la Comisión Estatal de Servicios Públicos de Ensenada (C.E.S.P.E.)

## I.1 Antecedentes

A través de los últimos años, los sistemas de Información se han transformado vertiginosamente, desde que la Informática se enfocó hacia el apoyo de la sistematización de las área del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nóminas, etc. lo cual originó inmediatamente mecanismos de control sobre éstos sistemas, "Posteriormente, el uso de la Informática cubrió las áreas de negocio en todos los niveles con productos y servicios muy variados, proliferaron las minicomputadoras o equipos departamentales, después llegaron las microcomputadoras o computadoras personales y entraron de lleno las redes locales, la integración empresarial a través de las telecomunicaciones y un gran número de componentes de tecnología." [2] Tal tecnificación del medio imposibilitó al responsable de Informática y a los Auditores de sistemas tradicionales seguir evaluando este campo con métodos y procedimientos anticuados.

Se hizo necesario un replanteamiento del fondo y forma de la Auditoría en Informática, un cambio que trata de dar a la Auditoría una dimensión más realista y adecuada a lo que hoy en día se requiere de la Auditoría en Informática. Lo cual les brindará a los negocios y a sus ejecutantes un sentimiento de satisfacción justificado por el entendimiento y compromiso que implica asegurar el uso correcto de los recursos de Informática para el logro de los objetivos empresariales.

Cabe mencionar que "la Auditoría en Informática nació en los Estados Unidos teniendo allí su proceso y evolución. En 1961 Dom Adams desarrolló el primer software de Auditoría (IBM'S 1401), en1963 El Centro de Entrenamiento ofrece los primeros Cursos de EDP (Electronic data Proscessing); en 1967 se desarrolla el software de Auditoría Auditape por Hasnkins and Sells, en 1969 Se funda la EDPAA (The Electronic Data Proscessing Aiditors Asociation), en 1971 se publica "Computers Controls Guideline" por CICA (Canadian Institute of Chartered Accountants ).

En 1976 se crea la EDPAF (Electrinic Data Proscessing Auditors Fundation), en 1978 El 21 de junio 1978, la Fundación de Auditores de Procesamiento Electrónico de Datos, anuncia oficialmente un programa de certificación Internacional de manera anual, con el fin de motivar a los Auditores de sistemas de información, a mantener su competitividad y monitorear los logros en los programas de mantenimiento y finalmente surge en nuestro País la Asociación Mexicana de Auditores en Informática (AMAI), con la finalidad de difundir los avances tecnológicos en esta área y con el objetivo de lograr así la actualización profesional continua." [3]

## I.2 Importancia de utilizar una metodología adecuada en la aplicación de auditorías en Informática.

Un alto porcentaje de los especialistas en áreas de investigación, planeación de Informática, desarrollo de sistemas y otras más, se apoyan en gran medida en tareas, actividades, revisiones, funciones, responsabilidades, etc., definidas previamente en un documento formal que contiene la metodología necesaria, con el fin de brindar a los responsables de dichas áreas un camino estructurado por donde llegar a los resultados que esperan obtener.

[2] Lic. Hernández Hernández E. Auditoría en Informática .1995.

La Auditoría en Informática como se mencionó anteriormente, debe ser respaldada por un proceso formal que asegure su previo entendimiento, ya que contar con un método garantiza que las cualidades de cada Auditor sean orientadas a trabajar en equipo para la obtención de productos de calidad estandarizados.

Es importante anotar que el uso de la metodología no garantiza por si sola el éxito de los proyectos de Auditoría en informática, es de gran importancia, más no lo único ya que son muchos los factores que se interrelacionan para lograr el objetivo de la función de Auditoria en Informática.

Desgraciadamente, la mayoría de las metodologías propuestas por diversos autores, son complejas y lentas, lo cual genera aún más apatía en su uso por los profesionistas en Informática, como por los directivos empresariales.

## I.3 Objetivo general

Desarrollo de una guía práctica para la aplicación de Auditorías en Informática con el propósito de que sea utilizada por los Profesionales en Informática en cualquier Institución.

## I.4 Alcance y limitaciones de la tesis.

Se realizará un estudio de diferentes metodologías para la aplicación de Auditorías en Informática, las cuales, serán tomadas como punto de referencia para el desarrollo de una guía práctica en la aplicación de Auditorías en Informática.

Se implantará la guía práctica en la Institución denominada Comisión Estatal de Servicios Públicos de Ensenada (C.E.S.P.E)

La limitación de esta tesis, es que su implantación o prueba se llevará a cabo sólo en la institución antes mencionada.

[3] M.A.E. Gutiérrez Peón F. Diplomado de Auditoría en Informática. Módulo I. P. 1y2

## I.5 Organización de la tesis.

La presente tesis está organizada como a continuación se describe:

El capítulo **uno** presenta una breve reseña del papel de las Organizaciones en la actualidad, la problemática que presenta el uso de sistemas e Informática, como apoya la Auditoría en Informática a los sistemas de información y la problemática de los sistemas de información automatizados.

El capítulo **dos** menciona e ilustra al lector de esta tesis con conceptos importantes sobre la estructura organizacional y los sistemas de información automatizados.

En el capítulo **tres** se menciona brevemente el entorno de la Auditoría en Informática.

El capítulo **cuatro** presenta una serie de conceptos y puntos relevantes e ilustrativos de los Auditores en Informática, así como un estudio comparativo de diferentes metodologías existentes par la realización de una guía propia.

En el capítulo **cinco** se expone la guía práctica para la aplicación de Auditorías en Informática y el desarrollo de cada una de sus etapas.

En el capítulo **seis** se presenta el caso práctico de la Auditoría en Informática aplicada al centro de cómputo de la Comisión Estatal de Servicios Públicos de Ensenada. C.E.S.P.E.

El capítulo **siete** expone las conclusiones generales de la tesis.

# CAPÍTULO II

# LA ESTRUCTURA ORGANIZACIONAL Y LOS SISTEMAS DE INFORMACIÓN EN FUNCIÓN DE INFORMÁTICA

## II.1 Concepto de Organización.

La palabra Organización proviene del vocabulario "ORGANON", lo que en Español conocemos mejor como "ORGANISMO", implicando:

- Partes y funciones diversas
- Unidades funcionales encaminadas a un fin común
- Coordinación, acciones complementarias que ayuden a los demás a construir, combinar.

Es decir, que Organización la podemos definir como :

- Arreglo de las funciones necesarias para lograr un objetivo y una indicación de la autoridad y responsabilidad asignada a quienes esté a cargo la ejecución de las mismas.
- Estructuración técnica de las relaciones entre funciones, niveles y actividades de los elementos materiales y humanos en un organismo social, con el fin de lograr su máxima eficiencia dentro de los planes y objetivos señalados.

La Organización es una entidad estructurada y relacionada con la misión, comportamiento, especialización y funciones que se orientan a objetivos estratégicos de una empresa. La Organización debe ser diseñada para que sea relativamente permanente y no se vea afectada por los cambios en su directiva.

Una característica clave de la Organización es que posee una estructura, lo que significa que dispone de un conjunto de medios prescritos y regularizados para coordinar sus actividades con el fin de alcanzar sus objetivos.

Todo tipo de Organización debe orientarse a sacar el mayor provecho de la especialización del personal en base a sus habilidades y conocimientos.

## II.2 Importancia de Auditar la Organización de la función de Informática.

Es de gran relevancia que "la alta dirección de cualquier Organización tiene que estar consciente de que la función de Auditoría se debe ejercer con el criterio básico de independencia personal jerárquica, es decir, que el desempeño de las actividades profesionales en el proceso de evaluación y control no debe verse afectado por aspectos emocionales ni de autoridad emanados de los responsables e involucrados en el momento de la Auditoría.

En la medida en que la dirección establezca políticas claras que especifiquen que la función del Auditor es asegurar el control y la seguridad de todos los elementos relacionados con la Informática y que responden a una necesidad de la alta dirección, a fin de contar con una entidad confiable y eficiente.

La falta de una posición Organizacional adecuada a las características específicas que la rodean, puede convertirla en foco de frustración e incertidumbre con el paso del tiempo." [4]

Algunos de los importantes **BENEFICIOS** generados al Auditar la función de Informática son:

- Optimización de la estructura Organizacional y sus funciones.
- Mejoramiento del proceso de planeación estratégica de Informática.
- Orientar al personal para que desarrolle su trabajo, bajo las mismas políticas y lineamientos.
- Optimización de los controles y políticas existentes.
- Brindar alternativas de mejoramiento para la toma de decisiones que se apoyan en sistemas de información.
- Recomendar acciones que permitan a la alta dirección evaluar la función de Informática para hacerla más rentable.

[4] Hernández Hernández, Auditoría en Informática, P.33

"Es importante recalcar que en la actualidad existe muy poca difusión y aún menor aceptación por parte de las empresas de la necesidad de contar con una función de Auditoría en Informática; sin embargo es factible pronosticar (con un alto grado de certidumbre) que el crecimiento acelerado de las inversiones y proyectos de Informática, donde se involucran todas las empresas, forzará que se tome una decisión al respecto, aunque a la Auditoría en Informática se le llame aseguramiento de calidad, evaluación de Informática o Auditoría de sistemas y sea ejercida por personal externo o interno de la empresa.

Una cantidad considerable de empresas aún cuestionan la rentabilidad y productividad de la función de Informática, prueba de ello son las empresas e instituciones donde la función de Informática depende de la dirección o las gerencias de recursos humanos, Finanzas, manufactura (empresas industriales), etc. y en algunos casos (que resultan increíbles en estos tiempos), de alguna jefatura de contabilidad o de los usuarios." [5]

## II.3 Concepto de Estructura Organizacional.

Es importante para el Auditor en Informática, (en la obtención de requerimientos previos de análisis) estudiar y dimensionar la estructura Organizacional y sus diferentes relaciones. Para ello debemos dejar bien claro que "La estructura Organizacional es el medio para distribuir las responsabilidades, proporcionando un marco de trabajo para la evaluación del desempeño y las operaciones, y proporciona mecanismos para procesar la información y ayudar a la toma de decisiones."[6]

[5] Hernández Hernández, Auditoría en Informática, P.36

### II.3.1. Principales componentes de la estructura de una Organización.

Los principales componentes de la estructura de una Organización son:

- La distribución de tareas y responsabilidades a los individuos. Aspectos de la estructura que entran en juego, aquí están en la forma de especialización diseñada en los puestos y en la discreción que se les da.
- La designación de relaciones formales de reportes, la determinación del número de niveles en las jerarquías y los ramos de control de los gerentes y supervisores.
- El agrupamiento de los individuos en secciones o departamentos, el agrupamiento de departamentos en divisiones y unidades más grandes, y el agrupamiento general de las unidades en el total de la Organización.
- El diseño de sistemas para asegurar la comunicación efectiva de la información, la integración de esfuerzo y la participación en el proceso de la toma de decisiones.
- La delegación de autoridad junto con los procedimientos asociados por medio de los cuales se vigila y evalúa el uso de la discreción.
- La provisión de sistemas para la evaluación de desempeño y las recompensas que ayudan a motivar más que alejar a los empleados.

Si alguno de estos componentes estructurales es deficiente, puede haber serias consecuencias para el desempeño de una Organización." [7]

[6] Child John, Organización: guía para problemas y práctica, P.38
[7] Child John, Organización: guía para problemas y práctica, P.18

## II.4 Niveles de apoyo del departamento de Informática a las Organizaciones.

El apoyo que el departamento de Informática proporciona a las Organizaciones, depende del nivel en que se encuentra dicho departamento dentro de la estructura Organizacional.

A continuación se presenta una clasificación de los diferentes niveles de apoyo que el departamento de Informática proporciona:

- Nivel inicial
- Nivel intermedio
- Nivel de madurez

| NIVEL | CARACTERÍSTICAS |
|---|---|
| INICIAL | • El nivel jerárquico de Informática puede llegar a estar en una jefatura o no existir.<br>• Regularmente los servicios ofrecidos al negocio son de cobertura departamental e igual importancia, algunos de ellos son:<br>- Desarrollo e implementación de sistemas<br>- Mantenimiento y/o manejo de los sistemas<br>- Compra/ instalación y reemplazo de equipo de cómputo.<br>- Compra de Software.<br>- Capacitación.<br>• El involucramiento de Informática en el proceso de planeación de negocio, así como en el de las estrategias es generalmente nulo, en gran medida se debe a factores como:<br>- Nivel jerárquico de Informática es bajo y si acaso sólo conocen la estrategia de la gerencia a la que le reportan.<br>- Los accionistas y directivos de la Organización, consideran a Informática como un factor operativo, "para ellos es un mal Necesario".<br>- El futuro de los negocios no depende según su punto de vista del apoyo de Informática.<br>• Personal de Informática tiene un rol meramente operativo. |

**Figura II.1** Nivel "Inicial" de apoyo del departamento de Informática a la Organización.

| NIVEL | CARACTERÍSTICAS |
|---|---|
| INTERMEDIO | • El nivel jerárquico de Informática puede llegar a estar en la subdirección, o gerencia.<br>• Regularmente los servicios ofrecidos al negocio son de mediana cobertura e igual importancia, algunos de ellos son:<br>- Planeación de Informática<br>- Desarrollo e implementación de sistemas<br>- Mantenimiento y/o manejo de los sistemas<br>- Admón. de redes locales y comunicaciones<br>- Soporte técnico / Capacitación<br>• El involucramiento de Informática en el proceso de planeación de negocio, así como el de las estrategias es regular, en gran medida se debe a factores como:<br>- Dependencia media en sistemas de información, cómputo y comunicaciones<br>- Los accionistas y directivos de la Organización, consideran a Informática como un factor táctico que apoyará a los niveles medios en sus procesos de negocio.<br>- El futuro de los negocios no puede relegar el manejo de información y tecnología de Informática a un sólo puñado de personas operativas incapaces de tomar decisiones .<br>• Personal de Informática tiene un rol de ejecutor de soluciones más que de consultor. |

**Figura II.2** Nivel "Intermedio" de apoyo del departamento de Informática a la Organización.

| NIVEL | CARACTERÍSTICAS |
|---|---|
| MADUREZ | • El nivel jerárquico de Informática puede llegar a estar en la dirección, subdirección o gerencia.<br>• Regularmente los servicios ofrecidos al negocio son de amplia cobertura e importancia, algunos de ellos son:<br>- Planeación estratégica de Informática / Consultores en tecnología<br>- Desarrollo e implementación de sistemas<br>- Mantenimiento y/o manejo de los sistemas<br>- Admón. de redes locales y de telecomunicaciones<br>- Investigación de nuevas tecnologías<br>- Administración de proveedores de Informática<br>- Soporte técnico / Asesorías<br>• El involucramiento de Informática en el proceso de planeación de negocio, así como el de las estrategias es alto, en gran medida se debe a factores como:<br>- Alta dependencia de la empresa en sistemas de información, cómputo y comunicaciones<br>- Los accionistas y directivos de la Organización, consideran a Informática como la plataforma de tecnología que apoyará de una manera más oportuna y eficiente los procesos del negocio.<br>- El futuro de los negocios no puede relegar el manejo de información y tecnología de Informática a un grupo de personas que carezcan de capacidad para tomar decisiones.<br>• Personal de Informática eficiente y dinámico (rol de consultor). |

**Figura II.3** Nivel "Madurez" de apoyo del departamento de Informática a la Organización.

## II.5 ¿Qué es información?

El primer aspecto que es importante aclarar es en relación con la diferencia que existe entre información y datos. Aunque muchas personas utilicen estos términos como sinónimos por falta de conocimientos o por costumbre, es radical que si existe diferencia entre uno y otro.

Empezaremos por considerar a los datos como los insumos para el sistema de información que los procesará posteriormente, es decir, se trata de magnitudes, cifras o relaciones por introducir para derivar la operación de un sistema. Los datos pueden tener una concepción diferente a numéricos y alfabéticos estrictamente hablando para la información, y es que pueden ser hechos, principios, mensajes sin evaluar.

La diferencia básica entre datos e información consiste en que los datos no son significativos como tales, sino hasta que son procesados y convertidos en una forma útil llamada información.

En consecuencia, mientras la información consta de datos, no todos los datos producen información específica que lleve a una adecuada toma de decisiones.

Se puede considerar que la información es el conocimiento derivado del análisis y proceso de los datos y que además debemos tomar en cuenta que la información obtenida en un proceso determinado puede servir como dato para otro.

Existen muchas concepciones de lo que es la información; se puede ver como el producto de un proceso, como elemento integrador de otro proceso en otros sistemas o subsistemas, como elemento de reducción de incertidumbre, como representación del conocimiento, como noticia, etc., Sin embargo la más importante puede ser la que considera como una comunicación que modifica los parámetros de una toma de decisiones.

En términos generales se debe tomar la información como un conocimiento importante que tiene su origen en el producto del procesamiento de algunas operaciones para saber algo a fondo, con el fin de:

1.- Lograr objetivos específicos 2.- Aumentar el entendimiento.

## II.6 Importancia de la información en las Organizaciones.

Sin importar cuál es el giro o actividad preponderante de una Organización, todas comparten una característica en común: la necesidad de obtener y analizar información, y emprender alguna acción basada en su interpretación. La información es necesaria para organizar cualquier tipo de actividad, es poder para quienes diariamente y a cada momento toman decisiones.

Todos los gerentes deben llevar a cabo ciertas tareas y funciones administrativas básicas con el fin de alcanzar los objetivos fijados, obviamente las metas que se persiguen son diferentes, pero en las labores administrativas son comunes para todos. En otras palabras, las funciones de planear, organizar, dirigir y controlar personal, deben cumplirlas todos los gerentes y administradores en una Organización. La forma en que los ejecutivos lleven a cabo éstas actividades determinan el éxito de la Organización y la forma en que éstas funciones se desarrollen, depende en gran parte del grado en que se estén cumpliendo las necesidades de información, esto se da porque cada función implica una toma de decisión y una decisión debe estar plenamente apoyada en una información que sea exacta, oportuna, compleja y concisa.

Si la información que tiene un gerente no posee alguna de estas características, se afectará la calidad de las decisiones que se tomen y en el mejor de los casos, no se tendrá el éxito que en otras circunstancias se hubiera logrado:

Una información de calidad en manos de personas que la pueden utilizar eficientemente, será el mejor respaldo para tomar decisiones además de una administración eficaz que conducirá al óptimo cumplimiento de las metas de la Organización. Por lo tanto la información constituye en un concepto general, el elemento que mantiene a una empresa unida y coordinada. Sin embargo existe la tendencia a no prestar mayor importancia a la información que se proporcione en el momento y lugar adecuado, en la cantidad y calidad apropiada, sólo reconocemos su importancia cuando su abastecimiento o la calidad se deteriora.

## II.7 ¿Qué es un sistema?

El concepto de sistema ha sido definido de muy diversas maneras por diferentes autores:

**ACKOFF:**

Lo define como un conjunto de elementos interrelacionados, cada uno de los cuales se relaciona directa o indirectamente con cada uno de los demás elementos, y en el que ningún subconjunto del mismo se encuentra desligado de los demás subconjuntos.

**ANGYAL:**

Plantea que un sistema es una forma de integrar partes.

**BERTALANFFY:**

Establece que un sistema puede ser definido por como un complejo de elementos interactuantes.

**CHURCHMAN:**

Dice que un sistema está formado por conjuntos de componentes que trabajan de común acuerdo para el logro de objetivo global del todo.

**HARE:**

Indica que el concepto de sistemas se refiere a una colección específica de variables y relaciones seleccionadas por el analista para un propósito particular.

**LANGEFORS:**

Define al sistema como una colección de objetos llamados partes que están correlacionados de alguna forma.

Como podemos observar la mayoría de los autores consideran que un sistema está formado por varias partes o componentes, los cuales interactúan uno de los otros. Esta interacción es la que da su esencia al sistema, ya que gracias a ella, se obtiene una nueva entidad distinta de la que forman las partes, e incluso, diferente del simple agregado de esos componentes.

Para generalizar diremos que sistema es un grupo de partes integradas con el propósito común de lograr algún o algunos objetivos.

## II.8 ¿Qué es un sistema de información?

Un sistema de información es "un conjunto de procedimientos ordenados que, al ser ejecutados, proporcionan la información para apoyar la toma de decisiones y el control en la Organización." [8]

### II.8.1 Funciones de los sistemas de información.

Las necesidades primordiales que deben cumplir los sistemas de información, generalmente son de dos grupos. Por un lado, deben APORTAR ELEMENTOS PARA LA TOMA DE DECISIONES y por otro, deben APOYAR LAS ACTIVIDADES OPERATIVAS DE LA ORGANIZACIÓN.

Estas dos funciones se complementan entre sí.

[8] Lucas, Henry C. Jr. Conceptos de los Sistemas de Información para la Administración, P.08

El aspecto sobre la toma de decisiones es uno de los principales argumentos para la introducción de los sistemas de información.

Sin embargo, pocos son los sistemas que llegan a operar en la práctica con este enfoque de manera adecuada y podemos decir que se debe a tres cuestiones:

a).- La infraestructura de datos necesaria sólo puede recopilarse y organizarse a través de un sistema de información de apoyo a las actividades operativas

b).- La naturaleza cambiante y poco estructurada de las decisiones, incluyendo el limitado análisis que generalmente se hace de la función de toma de decisiones al diseñar un sistema

c).- Los requerimientos de información de tipo externo, que se tiene para tomar muchas decisiones.

Totalmente los sistemas de información para la toma de decisiones se orientan a las funciones directivas de la Organización, donde se presentan principalmente decisiones no estructuradas y de carácter estratégico.

El aspecto del apoyo a las actividades operativas tiene un desarrollo empírico más amplio, aunque carece de un adecuado tratamiento teórico.

Esto significa que existe gran número de sistemas con este enfoque, pero las bases conceptuales y metodológicas para su diseño no están suficientemente desarrolladas.

"Los sistemas de información para apoyo operativo, en rigor también auxilian en la toma de decisiones pero su ámbito de acción es el nivel operativo en el área de decisiones estructuradas.

Por ejemplo: un sistema de nóminas es un sistema de información de apoyo operativo que permite calcular el pago de todos y cada uno de los empleados y entonces se tiene la decisión casi automática de la cantidad de capital que debe estar disponible para efectuar dicho pago". [9]

[9] Murdick Robert G. con Munson John C. Sistemas de Información Administrativa, P.423

Estas decisiones no son comparables de ninguna manera a las que tienen un carácter más amplio y estratégico. Por este motivo, es común llamar solamente a los expuestos en primer termino como sistemas de información para la toma de decisiones.

Los dos enfoques que se mencionaron deben plantearse en forma integral y coordinada, ya que no es posible contar con sistemas para toma de decisiones sin los sistemas de información operativa que recolecten y organicen datos.

Otro punto de importancia consiste en que un sistema de apoyo operativo pierde su perspectiva organizativa si no se contempla como un elemento del sistema para la toma de decisiones.

## II.9 Sistema de información basado por computadora.

"Los sistemas de información existieron mucho antes del desarrollo de las computadoras electrónicas. Sin embargo, la explosión de información y la necesidad de procesar grandes cantidades de datos para extraer pequeñas cantidades de información han contribuido a incrementar la importancia de los sistemas informativos basados en computadora. Naturalmente, dichos sistemas existen gracias a la alta velocidad de procesamiento de las computadoras." [10]

[10] Lucas Henry C. Jr. Conceptos de los Sistemas de Información para la Admón., P.09

Un sistema de información tiene cinco componentes básicos, como se muestra en la siguiente figura. En un sistema manual los seres humanos son los que ejecutan esas cinco funciones básicas, mientras que en un sistema basado en computadoras, el equipo es el que ejecuta esas mismas funciones. En cualquiera de esos tipos de sistemas, esas funciones básicas son las siguientes:

1.- Entrada de los datos al sistema.
2.- El procesamiento de los datos (el ordenamiento de los datos de entrada y los archivos de procesamiento),
3.- Mantenimiento de los archivos y registros,
4.- Desarrollo de los procedimientos que digan cuáles datos se necesitan, y cuándo y dónde se obtienen, y cómo se usarán, y también el suministro de instrucciones de rutinas que deberá seguir el procesador, y
5.- Preparación de los informes de salida.

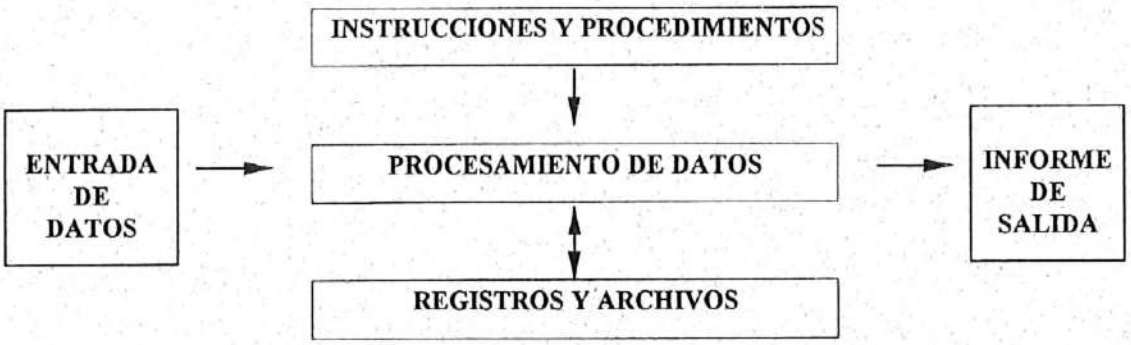


**Figura II.4** Componentes básicos de los sistemas de información.

### II.9.1 Tipos de sistemas de información basados en computadora.

Es útil conocer cuál es la clasificación de estos, sobre todo, de acuerdo a la tecnología empleada.

**1.- SISTEMA SIMPLE:** Este es un sistema por lotes (batch) en donde todas las entradas al sistema se procesan en un momento determinado para producir la salida o el resultado deseado. Los datos de entrada se almacenan y emplean para actualizar periódicamente los archivos diaria, semanal o mensualmente, en este tipo de sistema los datos están a menudo retrasados pero el procesamiento es muy económico.

**2.- PREGUNTA SIMPLE:** En este sistema, los datos son procesados para su actualización en lote pero el acceso a la información puede estar en "línea", este sistema tiene una ventaja con el anterior, porque se tiene a la disponibilidad de datos en forma interactiva para su consulta, aunque la captura de datos y su actualización será en batch.

**3.- PREGUNTA Y REGISTRO:** Este sistema es similar al anterior en cuanto a su tipo de proceso de datos (que es por lotes) y a su disponibilidad de datos para consulta en forma interactiva. La diferencia radica en la manera como se capturan los datos, porque se condiciona la terminal de teleproceso para que capte entradas de datos en un archivo temporal que posteriormente se emplea para actualizar el sistema.

**4.- INTEGRAL EN LÍNEA:** Es un sistema de acceso, actualización y consulta directa en línea, modificando los archivos cuando los datos son ingresados por medio de las terminales. Obviamente estos sistemas requieren de una tecnología más avanzada y costosa.

**5.- MANDO Y CONTROL:** Son sistemas que deben trabajar en tiempo real en donde los datos que se están ingresando deben ser actualizados inmediatamente para poder controlar correctamente el flujo de las operaciones y así tener una retroalimentación que les permita asegurar los resultados óptimamente.

| TIPOS | CAPTURA | PROCESO | ACCESO |
|---|---|---|---|
| Sistema simple | Lote | Lote | Lote |
| Pregunta simple | Lote | Lote | Consulta en línea |
| Pregunta y registro | En línea | Lote | Consulta en línea |
| Integral en línea | En línea, tiempo compartido | En línea, tiempo compartido | Consulta/activa tiempo compartido |
| Mando y control | En línea, tiempo real | En línea, tiempo real | Consulta/activa tiempo real |

**Fig. II.5** Algunos tipos de Sistemas de Información basados en computadora.

## II.10 Comparación de los sistemas de información con los sistemas de información basados en computadora.

"La siguiente tabla presenta alguna de las diferencias entre sistema de información (comúnmente llamados sistemas de información manuales) y los basados en computadora". [11]

| | Manual | Computadora |
|---|---|---|
| Comprensión de la tecnología | Fácil: requiere el procesamiento humano ordinario o una operación sencilla de tabulación. | Difícil: tecnología arbitraria y de difícil comprensión desde el punto de vista del usuario. |
| Establecimiento de normas | Muy informal y susceptible de ser cambiada. | Proceso formal que requiere gran precisión y detalle; debe especificarse por anticipado. |
| Administración del proyecto | Es tarea sencilla establecer los procedimientos. | Resulta difícil concluirlo a tiempo y sin salirse del presupuesto. |
| Conversión e instalación | Generalmente un proceso fácil, que comprende pocos procedimientos nuevos. | Puede ser una tarea laboriosa que requiere cambios y capacitación importantes. |
| Repercusión en la empresa | Mínima, las más de las veces | Puede ser importante; implica cambios de desempeño y Organizacionales. |
| Flexibilidad | Generalmente fácil de cambiar con rapidez. | A menudo muy difícil de cambiar; los cambios pueden ser costosos y requerir largo tiempo. |

**Figura II.6** Comparación de los sistemas de Información Manuales y los basados en computadora.

[11] Lucas Henry C. Jr. Conceptos de los Sistemas de Información para la Admón. P.09

# CAPÍTULO III
# LA AUDITORÍA EN INFORMÁTICA Y SU ENTORNO.

## III.1 Entorno de la Auditoría en Informática.

Antes de conocer que es lo que rodea a la Auditoría en Informática primero conoceremos su concepto.

**Auditoría en informática** :

*"Es la revisión y evaluación de los controles, sistemas, procedimientos de Informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la Organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones."* [12]

Las actividades de un negocio tienen un efecto directo sobre sectores específicos de la sociedad; de igual manera los hechos y actividades externos al negocio tienen un grado de impacto en el mismo; el medio puede marcar las pautas y caminos estratégicos en los diferentes aspectos que deben contemplar un negocio y los factores que lo afectan pueden ser económicos, políticos, culturales, tecnológicos, ecológicos, sociales y organizacionales.

Dado que la Auditoría en Informática es un proceso básico de evaluación y control en el uso de los recursos tecnológicos para el logro de las estrategias, debe de contemplar el entendimiento del entorno del negocio como parte de sus actividades primarias.

Para los negocios es importante evaluar en forma constante cada factor externo que predomine o los afecte en forma trascendente, con la finalidad de instituir las acciones necesarias para minimizar el impacto negativo o sacar ventaja estratégica del mismo.

[12] Echenique García José Antonio. Auditoría en Informática . Pág. 16.

Existen funciones como Planeación, Auditoría, Controlaría y Auditoría en Informática que verifican y aseguran el cumplimiento formal de las estrategias definidas por la Organización. Al hablar de factores externos que pueden afectar a la organización pueden ser como :

La reducción de las cifras en tres dígitos las cuales son emanadas de decretos gubernamentales, auge en el uso de la tecnología de comunicaciones vía satélite como una acción para obtener ventajas competitivas, el tratado de libre comercio, etc.

No contar con las áreas de aseguramiento y verificación orilla a las empresas a vivir en una constante incertidumbre , ya que los problemas o deficiencias pueden aparecer en cualquier momento.

### III.1.1 Entorno en la Informática.

La función de Informática debe estructurar sus servicios y proyectos con base en los requerimientos específicos del negocio, apoyándose en la tecnología de vanguardia que domina el mercado, así como en las tendencias de la misma . El grado de apoyo que debe buscar en el medio tecnológico dependerá en gran medida de la orientación y justificación que se le asigne.

No todo lo que se ofrece en el mercado como estándares de soluciones tecnológicas garantiza el desempeño eficiente de la función de Informática en una Organización; el Auditor en informática debe verificar la existencia de un análisis costo/beneficio en cada proyecto de inversión orientado a la adquisición de nueva tecnología o estándares par el uso y manejo de la misma. Además la Auditoría en Informática debe de mantener un proceso de seguimiento de los recursos de tecnología, metodologías, técnicas , procedimientos y políticas de informática que aseguren calidad y productividad en esa área.

El medio informático sufre cambios continuos en algunos de sus elementos ya sea en software, hardware, telecomunicaciones etc. En los últimos años el entorno de la Informática ha sido uno de los campos con mayor ritmo de crecimiento en todas sus áreas de acción por lo que hoy en día podemos contar con :

- Mejores equipos de cómputo, ya que cuentan con características nunca antes proporcionadas, como colectividad y escalabilidad .
- Lenguajes de programación y paquetes de Software mas flexibles y dinámicos .
- Innovaciones tecnológicas en telecomunicaciones, ya que se puede transmitir voz, datos e imágenes, con esto se ha alcanzado a enlazar diferentes empresas con clientes y proveedores a través de redes locales (LAN), redes metropolitanas (MAN) y redes abiertas (WAN), se ha obtenido la capacidad de manejar grandes volúmenes de información, velocidad de transmisión y protección de los datos con la utilización del cable coaxial y la tecnología de redes digitales." [13]
- Metodología, técnicas y herramientas para la administración de la función de informática y la planeación y desarrollo de sistemas que han venido formalizándose y apegándose a los estándares aceptados a nivel nacional e internacional, lo que ha sido un factor de suma utilidad para el desempeño eficiente de las tareas y servicios inherentes a la Informática y a la Auditoría en informática.
- La integración de especialidades profesionales ( Ingeniería , Auditoría, Informática, etc.) en Asociaciones profesionales reconocidas formalmente a nivel nacional, como la Asociación Mexicana de Auditores en Informática (AMAI) e internacional, como la Auditors Association, Inc. (EDP) entre otras . Dichas asociaciones proporcionan, la oportunidad a las instituciones y organizaciones privadas y de gobierno de tener contacto directo y oportuno con los conocedores o impulsores de las tendencias dominantes del medio en sus diferentes áreas.

[13] Hernández Hernández Enrique Auditoría en Informática . P. 24

Es importante que la función de Auditoría en Informática tome conciencia del entorno que la rodea y se mantenga actualizada mediante accesos a bases de datos nacionales e internacionales, conferencias, periódicos o revistas especializadas, incorporándose a asociaciones o colegios especializados, contacto permanente con proveedores líderes de productos y servicio de la tecnología de Informática, análisis permanentes de los procesos básicos del negocio y sus competidores.

### III.1.2 Objetivos del Auditor en Informática al estudiar el entorno y su impacto en la Organización.

La finalidad principal del Auditor es evaluar y dar seguimiento oportuno al conjunto de proyectos de Auditoría en Informática que serán ejecutados en un determinado plazo con el fin de apoyar directamente o indirectamente las estrategias del negocio, considerando los diversos factores internos y externos que se relacionan con la Organización.

La Auditoría en Informática se enfoca en evitar la interrupción de las operaciones de la organización y, al mismo tiempo, busca salvaguardar los activos relacionados de manera natural con el campo de acción de la Informática.

Los Auditores en Informática deben dirigir la participación directa del personal de Informática y de los usuarios involucrados durante la Auditoría, además se debe coordinar con el responsable de la Auditoría tradicional, la alta dirección y con el responsable de Informática mediante reuniones formales y periódicas para el logro de los objetivos.

# CAPÍTULO IV
# DIFERENTES METODOLOGÍAS Y TÉCNICAS USADAS PARA EL DESARROLLO Y APLICACIÓN DE AUDITORÍAS EN INFORMÁTICA

"Al igual que otras funciones en el negocio la Auditoría en Informática efectúa sus tareas y actividades mediante una *METODOLOGÍA."*[14] Por lo que los Auditores basan el desarrollo de Auditorías en Informática en metodologías que deben ser comprendidas por todos ellos y complementarlas con elementos propios de la función de Auditoría en informática.

Lo anterior se facilita si la metodología que se elija está orientada a una ejecución armoniosa y planeada para cada una de las tareas y actividades involucradas para la correcta aplicación de la Auditoría en Informática; con la finalidad de brindar a los responsables un camino estructurado por donde llegar a los resultados que espera la empresa.

Existen diferentes metodologías, técnicas y herramientas para la aplicación de Auditorías en Informática, por lo que hacer una elección perfecta es casi imposible; puesto que cada empresa aún perteneciendo al mismo giro o actividad y compartiendo algunas características, siempre serán distintas entre si. Por lo que los Auditores en Informática tienen la delicada tarea de hacer la elección correcta utilizando su experiencia, criterio, conocimientos y dominio de aspectos complementarios de las metodologías como lo son las técnicas, herramientas, habilidades personales, conocimientos técnicos y administrativos entre otros.

El propósito principal del presente capítulo es el de plantearnos un camino digerible y práctico para desarrollar una *GUÍA PRÁCTICA PARA LA APLICACIÓN DE AUDITORÍAS EN INFORMÁTICA* realizando un estudio de diferentes metodologías existentes.

[14] Hernández Hernández, Enrique Auditoria en informática Pág. 16

En dicho estudio, obtendremos elementos suficientes para que aunados a las consultas bibliográficas, plantear una guía propia la cual utilizaremos en la aplicación de una Auditoría como ya lo mencionamos anteriormente, al centro de cómputo de la C.E.S.P.E.

Es importante señalar que las metodologías que aquí presentamos no son las únicas que estudiamos y fueron elegidas con el propósito de presentarlas como un ejemplo representativo de las que encontramos para realizar nuestro trabajo.

Pero antes de entrar de lleno al estudio, revisaremos algunos aspectos importantes sobre las metodologías, los Auditores y la Auditoría en Informática, para contar con un panorama más amplio y así, obtener más elementos que nos ayuden a formarnos un mejor criterio.

## IV. 1 Algunos conceptos y puntos básicos de las metodologías y Auditores en Informática.

### IV.1.1 Metodología.

*" Es un conjunto de etapas (fases o módulos) formalmente estructurados, de manera que brinden parámetros de acción en el desarrollo de proyectos. "* [15]

[15] Hernández Hernández, Enrique Auditoría en Informática Pág. 71,72.

### IV.1.2 Principales aspectos a considerar al elegir una metodología.

1.- Que la metodología a elegir esté enfocada al área de Auditoría en Informática.

2.- Que contemple el *que hacer, quien debe hacerlo y cuando debe hacerse.*

3 .- Que esté bien documentada.

4.- Que cuente con los siguientes puntos:

- Un panorama general de la metodología.
- Equipos de trabajo sugeridos.
- Etapas de la metodología.
- Tareas de cada etapa.
- Secuencia de las etapas y de las tareas.
- Responsables e involucrados en cada etapa y tarea.
- Revisiones formales e informales por cada etapa y cada tarea.
- Duración estimada de cada etapa y tarea.

### IV.1.3 Algunas ventajas que generan el uso de metodologías en la aplicación de Auditorías en informática.

- Se elimina el proceso informal del trabajo.
- Los recursos orientan sus esfuerzos a la obtención de productos de calidad, con características y requisitos comunes para todos los responsables.
- Las tareas y productos terminados de los proyectos se encuentran definidos y formalizados en un documento al alcance de todos los Auditores en Informática.
- Se facilita en alto grado la Administración y seguimiento de los proyectos, pues la metodología obliga a la planeación detallada de cada proyecto bajo criterios estándares.
- Facilita la superación profesional y humana de los individuos, ya que orienta los esfuerzos hacia la especialización, responsabilidad, estructuración y depuración en las funciones del Auditor en Informática.

- Es un complemento clave en el desarrollo de cada individuo, ya que su formal seguimiento, aunado a las habilidades, normas y criterios personales ayuda al cumplimiento exitoso de los proyectos de Auditoría en Informática.
- El proceso de capacitación o actualización en el uso de un proceso metodológico es más ágil y eficiente, dado que se trabaja sobre tareas y productos terminados perfectamente definidos.

### IV.1.4 Técnicas.

*" Son el conjunto de pasos ordenados lógicamente para apoyarse en la terminación (como hacerlo) de todas las acciones o tareas estimadas en el proyecto emanado de la metodología."* [16]

### IV.1.5 Diferentes técnicas para el desarrollo de Auditorías en Informática.

Existen muchas técnicas para el desarrollo de la Auditoría en Informática, sólo las mencionaremos ya que su aplicación es muy variada y adaptable a las necesidades del Auditor.

- Existen técnicas que podemos utilizar en las diferentes etapas de las metodologías.

Como lo son:

Técnicas para la recopilación de Información.

Técnicas para la evaluación de los sistemas.

Técnicas para la evaluación del análisis.

Técnicas para la evaluación del diseño lógico del sistema.

Técnicas para la evaluación del desarrollo de sistemas.

Técnicas para el control de proyectos.

Técnicas para la interpretación de la información etc.

[16] Hernández Hernández. Enrique, Auditoría en informática Pág. 13.

### IV.1.6 Herramientas.

*" Es el conjunto de elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica."* [17]

Algunas de las herramientas de Auditoría son:

- Entrevista.
- Cuestionario.
- Muestreo Estadístico.
- Diagrama de flujo y otras.

### IV.1.7 Procedimientos de la Auditoría.

*Es la agrupación de diversas técnicas basándose en programas de Auditoría. El auditor debe aplicar los procedimientos de Auditoría de acuerdo a las circunstancias específicas del trabajo con la oportunidad y alcance que juzgue necesario en cada paso.*

### IV.1.8 Obligaciones del Auditor en Informática.

La Auditoría en Informática se desarrolla en función de normas, procedimientos y técnicas definidas por Institutos establecidos a nivel Nacional e Internacional. Por lo que el Auditor en Informática tiene la obligación de apegarse a las normas de Auditoría, así como, estar familiarizado con el código de ética de Auditores en Informática. (Ver Anexo 1,2.)

### IV.1.9 Perfil del Auditor.

Los requisitos que debe cumplir un profesionista para encajar en el perfil del Auditor son:

- Independencia : de criterio, pensamiento y objetividad.
- Agresividad: Fuerza y empuje para el trabajo aún, en un ambiente negativo.
- Creatividad: Desarrollar modelos y herramientas, ver el cómo hacer las cosas.
- Juicio: Juzgar siempre con elementos válidos y no dejarse llevar sin analizar antes.
- Técnica: Capacidad lógica.
- Facilidad para expresarse.
- Tacto: Poder enfrentar las situaciones delicadas.
- Discreción: En el manejo de la información confidencial.

### IV.1.10 Conocimientos y habilidades con los que debe contar un Auditor.

- Profesionalismo como Auditor.
- Habilidad para revisar y evaluar el control Interno de las funciones de Informática y recomendar los procedimientos de Auditoria requeridos.
- Entender el diseño de sistemas y su operación.
- Conocimientos de lenguajes de programación y las técnicas de programación.
- Estar familiarizado con los sistemas operativos y con el Software en general.
- Habilidad para identificar y reconciliar problemas.
- Habilidad para establecer un puente de comunicación entre la función de Auditoría y la de Informática.
- Saber cuando solicitar la ayuda de un experto en Informática para apoyar su función de Auditoría en Informática.

[17] Hernández Hernández , Auditoría en Informática . Pág. 16

## IV.2 *DIFERENTES METODOLOGÍAS EXISTENTES.*

### IV.2.1 Primer metodología.

- Esta metodología fue realizada por José Antonio Echenique García y dada a conocer a través de su libro titulado "Auditoría en Informática", donde describe paso a paso como evaluar la función de Informática desde los siguientes puntos:
- La parte administrativa del departamento de Informática.
- Los recursos materiales y técnicos del área de Informática.
- Los sistemas y procedimientos y la eficiencia de su uso y su relación con las necesidades de la Organización.

*INICIO DE LA METODOLOGÍA:*

**I PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA.**

Dentro de la Auditoría en general, la planeación es uno de los pasos más importantes, ya que una inadecuada planeación repercutirá en una serie de problemas, que pueden provocar que no se cumpla bien con la Auditoría.

Para lograr una buena planeación, lo primero que se requiere es obtener información general de la Organización y de la función de Informática a evaluar, para ello se requiere de un análisis preliminar.

**1.- Investigación preliminar.**

Para poder analizar y dimensionar la estructura por Auditar se debe solicitar:

A nivel Organización total.

- Objetivos a corto y a largo plazo.
- Manual de la organización.
- Antecedentes o historia del organismo.
- Políticas generales.

A nivel área de Informática:

- Objetivos a corto y largo plazo.
- Manual de la Organización del área que incluya puestos, funciones, niveles jerárquicos y tramos de mando.
- Manual de políticas, reglamentos internos, y lineamientos generales.
- Número de personas y puestos en el área.
- Procedimientos administrativos del área.
- Presupuestos y costos del área.

## RECURSOS MATERIALES Y TÉCNICOS.

Solicitar documentos sobre los equipos, número de ellos localización y características.

- Estudios de viabilidad.
- Número de equipos localización y las características (de los equipos instalados, por instalar y programados).
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, venta y servicios de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión y ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

**SISTEMAS.**

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos y salida.
- Salidas.
- Fecha de instalación de los sistemas.
- Proyectos de instalación de nuevos sistemas, en el momento de hacer la planeación de la Auditoría o bien su realización.

**2.- PERSONAL PARTICIPANTE:**

Una de las parte más importantes dentro de la planeación de Auditoría es el personal que deberá participar.

El número de personas que participarán en las Auditorías es dado en función de las dimensiones de la Organización, de los sistemas y de los equipos, lo que se deberá considerar, son las características del personal que habrá de participar en la Auditoría.

El personal deberá estar debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos(eficiencia) y se le retribuya o compense justamente por su trabajo.

El grupo debe de estar formado por:

Personal asignado por la Organización, personas asignadas por los usuarios, para completar el grupo de los colaboradores directos en la realización de la Auditoría se debe tener personas con las siguientes características:

- Técnico en Informática.
- Conocimientos de Administración, Contaduría y Finanzas.
- Experiencia en el área de Informática.
- Experiencia en operación y análisis de sistemas.
- Conocimientos y experiencia en Psicología Industrial.
- Conocimientos de los sistemas más importantes.

## II AUDITORÍA DE LA FUNCIÓN DE INFORMÁTICA

### 1. Recopilación de la información organizacional.

Una vez elaborada la planeación de la Auditoría, la cual servirá como plan maestro de tiempos, costos y prioridades, y como medio de control de la Auditoría, se debe empezar la recolección de la información.

Se procederá a efectuar la revisión sistematizada del área a través de la observación y entrevistas de fondo en cuanto a:

**A) Estructura Orgánica**

- Jerarquías (Definición de la autoridad línea, funcional y de asesoría)
- Estructura Orgánica.
- Funciones.
- Objetivos.

**B) Se deberá revisar la situación de los recursos humanos.**

**C) Entrevistas con el personal de procesos electrónicos**:

a) Jefatura.

b) Análisis.

c) Programa

d) Operadores.

f) Capturistas

**D) Se deberá conocer la situación presupuestal y financiera en cuanto a** :

- Presupuesto.
- Recursos financieros.
- Recursos materiales.
- Mobiliario y equipo.

**E) Se hará un levantamiento del censo de recursos humanos y análisis en cuanto a :**

- Número de personas y distribución por áreas
- Denominación de puestos.
- Capacitación.
- Conocimientos.
- Escolaridad.
- Experiencia profesional.
- Antigüedad.
- Historia del trabajo.
- Salario y conformación.
- Movimientos salariales.
- Índice de rotación del personal.
- Programa de capacitación (vigente y capacitación dada en el último año).

**F) Por último, se deberá revisar el grado de cumplimiento de los documentos administrativos.**

- Normas y políticas.
- Planes de trabajo.
- Controles.
- Estándares y Procedimientos.

*La información nos servirá para determinar:*

- Si las responsabilidades en la Organización están definidas adecuadamente.
- Si la estructura Organizacional está adecuada a las necesidades.
- Si el control Organizacional es el adecuado.
- Si se tienen objetivos y políticas adecuadas, si están vigentes y están bien definidas.
- Si existe documentación de las actividades, funciones y responsabilidades.
- Si los puestos se encuentran definidos y señaladas sus responsabilidades.
- Si el análisis y descripción de puestos están de acuerdo con el personal que los ocupa.
- Si se cumplen los lineamientos Organizacionales.
- Si el nivel de salarios está comparado con el mercado de trabajo.
- Si los planes de trabajo concuerdan con los objetivos de la empresa.
- Si se cuenta con los recursos humanos necesarios que garanticen la continuidad de la operación o se cuenta con los indispensables.
- Si se evalúan los planes y se determinan las desviaciones.

## 2.- EVALUACIÓN DE LA ESTRUCTURA ORGÁNICA.

Para lograr el objetivo de evaluación de la estructura orgánica se deberá solicitar el manual de Organización de la dirección del cual deberá comprender como mínimo.

- Organigrama con jerarquías.
- Funciones
- Objetivos y políticas.
- Análisis, descripción y evaluación de los puestos.
- Manual de procedimientos.
- Manual de formas.
- Instructivos de trabajo o guías de actividad.

*También se deben solicitar:*

- Objetivos de la dirección.
- Políticas y normas de la dirección.

### 2.1 Estructura orgánica. ( *La información se recopila mediante cuestionarios.*)

2.1.1 Bases jurídicas.

2.1.2 Niveles jerárquicos.

2.1.3 Departamentalización.

2.1.4 Puestos.

2.1.5 Expectativas

2.1.6 Autoridad.

**2.2 Funciones**.

2.2.1 Existencia.

2.2.2 Coincidencias.

2.2.3 Adecuadas.

2.2.4 Cumplimiento.

2.2.5 Apoyos.

2.2.6 Duplicidad.

**2.3 Objetivos.**

2.3.1 Existencia

2.3.2 Formales.

2.3.3 Adecuados

2.2.4 Cumplimiento.

2.3.5 Actualización.

**2.4 Análisis de Organizaciones.**

Si no existe un organigrama en la Organización, el Auditor elaborará uno que muestre el actual plan de Organización, ya que facilita el estudio y da una imagen general de la Organización.

*Criterios para analizar organigramas:*

a) Agrupar funciones similares.

b) Agrupar funciones que sean compatibles.

c) Localizar la actividad cerca de la función a la sirva.

d) Localizar la actividad cerca o dentro de la función mejor preparada para realizarla.

f) Separar las funciones de control y aquellas que serán objeto del mismo.

g) Ningún puesto debe tener dos o mas líneas de dependencia jerárquica.

## 3.- EVALUACIÓN DE LOS RECURSOS HUMANOS.

Se deberá obtener información sobre la situación del personal del área.

Para obtener información se realizan cuestionarios sobre los siguientes aspectos:

3.1 Desempeño y comportamiento.

3.2 Capacitación

3.3 Supervisión.

3.4 Limitantes.

3.5 Condiciones de trabajo.

3.6 Remuneraciones.

3.7 Organización del trabajo.

3.8 Desarrollo y motivación.

## 4.- Entrevista con el personal de Informática

## 5.- Situación presupuestal y financiera.

5.1 Presupuestos.

5.2 Recursos financieros y materiales.

5.2.1 Recursos financieros.

5.2.2 Recursos materiales.

5.2.3 Mobiliario y equipo.

## III EVALUACIÓN DE LOS SISTEMAS

1. Evaluación de sistemas.
2. Evaluación del análisis.
3. Evaluación del diseño lógico del sistema.
4. Evaluación del desarrollo del sistema.
5. Control de proyectos.
6. Control de diseño de sistemas y programación.
7. Instructivos de operación.
8. Forma de implantación.
9. Equipo y facilidades de información.

## IV EVALUACIÓN DEL PROCESO DE DATOS Y DE LOS EQUIPOS DE CÓMPUTO.

1. Controles.

1.1 Control de datos fuente y manejo de cifras de control.

1.2 Control de operación.

1.3 Control de salida.

1.4 Control de asignación de trabajo.

1.5 Control de medios de almacenamiento masivo.

1.6 Control de mantenimiento.

2. Orden en el centro de cómputo.
3. Evaluación de la configuración del sistema de cómputo
4. Productividad.

## V EVALUACIÓN DE LA SEGURIDAD.

1. Seguridad lógica y confidencial.
2. Seguridad en el personal.
3. Seguridad física.
4. Seguros.
5. Seguridad en la utilización del equipo.
6. Procedimientos de respaldo en caso de desastre.
7. Condiciones, procedimientos y controles para otorgar soporte a otras instituciones.

## V I INTERPRETACIÓN DE LA INFORMACIÓN.

1. Técnicas para la interpretación de la información.
    - 1.1 Análisis critico de los hechos.
    - 1.2 Metodología para obtener el grado de madurez del sistema.
    - 1.3 Uso de diagramas.
2. Evaluación d los sistemas.
3. Evaluación de los sistemas de información.
4. Controles.
5. Presentación.

### IV.2.2 Segunda metodología.

Esta metodología es propuesta por Mancera S.C, en su Curso/Taller de Auditoría en Informática .

**Auditoría de controles generales del funcionamiento de los sistemas de información automatizados de las áreas de Informática.**

*Evaluación del funcionamiento de los sistemas de información automatizados.*

*A través de controles..*

- El objetivo de ésta metodología es identificar la existencia y funcionalidad de mecanismos de control sobre las funciones propias del área de Informática.

- ***Metodología para la evaluación de Controles generales.***

***Pasos a seguir:***

*1.- Realizar un repaso preliminar de controles.*

*2.- Documentar los controles generales.*

*3.-Probar los controles generales.*

*4.- Evaluar la eficiencia de los controles generales.*

**Áreas de revisión de controles generales.**

*A)* Controles de la organización.

b) Administración de los recursos computacionales

c) Controles de desarrollo y mantenimiento de los sistemas.

D) Controles de operación de centros de cómputo.

e) Controles de seguridad lógica y física.

***A)* Controles de la organización.**

Se debe evaluar que los objetivos de control se dirijan a lograr una adecuada segregación de funciones, asignación de responsabilidades, rotación de deberes y supervisión .

Los procedimientos de control deberán asegurar el logro de los objetivos de control.

1.- Organigramas.

2.- Niveles de responsabilidad y autoridad.

3.- Manuales de organización.

4.- Definición de la división de funciones:

- Area de sistemas - usuarios.
- Programación - operación.
- Control - Operación.
- Control - Programación.
- Control - personal.

**B) Administración de los recursos computacionales .**

Se debe de evaluar que los objetivos de control estén dirigidos al logro de una adecuada planeación tanto de los recursos materiales como los recursos humanos y su administración de la estandarización de procedimientos administrativos y de sistemas.

**Procedimientos de control a evaluar:**

1.- La metodología para la selección y adquisición de equipos de cómputo.
2.- Que los usuarios cumplan con el trabajo y lo notifiquen.
3.- Manuales de políticas y procedimientos.
4.- Planes a corto largo y mediano plazo de nuevos sistemas.
5.- Planes de capacitación para el personal
6.- Control presupuestal del área.
7.- Supervisión adecuada para el área.

**C) Controles de desarrollo y mantenimiento de los sistemas.**

Se debe de evaluar que los controles estén dirigidos a lograr que las transacciones sean manejadas apropiadamente y que los datos sean manejados de una forma precisa y segura en la información, para lo cual, se deben de desarrollar las siguientes actividades.

**Procedimientos de control a evaluar:**

1.- Calendarización de las proyectos de desarrollo de los de sistemas.

2.- Supervisión de los trabajos.

3.- Procedimientos para la asignación de prioridades.

4.- Realización de bitácoras de los avances de los proyectos.

5.- Definición de las cargas de trabajo y asignación de las tareas.

6.- Supervisiones del control de fallas y de mantenimientos.

7.- Utilización de estándares para errores de Hardware, Software, Aplicaciones e Instalaciones

**D) Controles de operación de centros de cómputo.**

Evaluar que los controles estén dirigidos a una adecuada implantación de sistemas a través de un adecuado desarrollo de los mismos.

- **Procedimientos de control a evaluar.**

1.- Control de la metodología de análisis, diseño, programación, prueba, implantación de sistemas, documentación y capacitación de usuarios.

2.- Metodología para el mantenimiento de los sistemas.

3.- Segregación de funciones en la construcción de los sistemas.

**E) Controles de seguridad lógica y física:**

Se debe evaluar que los controles estén dirigidos a garantizar la operación continua de los sistemas, equipos y la seguridad física y lógica de los mismos.

**Procedimientos de control a evaluar.**

1.- Independencia Física con otras áreas de la organización.

2.- Acceso restringido al área de Informática.

3.- Equipo de detección y extinción de fuego.

4.- Que no exista riesgo de inundaciones.

5.- Contar con plan de contingencias efectivo.

6.- Pólizas de seguros adecuadas.

7.- Equipo no "BREACK", sistemas de energía ininterrumpida.

8.- Respaldos fuera de las instalaciones de cómputo.

9.- Sistemas de passwords de acceso a los equipos y a los sistemas.

10.- Detección de accesos no autorizados.

### IV.2.3 *Tercera metodología.*

Esta metodología es propuesta por Mancera S.C.

*Primera etapa.*

**Evaluación del procesamiento electrónico de datos *(P.E.D).***

El objetivo de ésta etapa es la de identificar la existencia y funcionalidad de mecanismos de control sobre las funciones propias del área de sistemas.

*Etapa No.2*

**EVALUACIÓN DE LAS APLICACIONES.**

En ésta etapa se identifica, analizan y evalúan las aplicaciones sustantivas, sus características y procesos actuales a fin de emitir un informe de mejoramiento.

*Etapa No.3*

- **EVALUAR LA COLECCIÓN DE DATOS.**

  Las actividades de ésta etapa se orientan a identificar los datos críticos, su asociación con las aplicaciones y los procedimientos de Administración de datos.

*Etapa No.4*

**EVALUAR LA TECNOLOGÍA DE INFORMACIÓN.**

- En ésta etapa se identifican los componentes existentes de tecnología, como son procesadores , componentes de Hardware y su relación con el software.

*Etapa No. 5*

**REVISIÓN Y APROBACIÓN.**

- En ésta etapa se revisan los resultados y productos de evaluación , se realizan los riesgos con el fin de tomar acciones apropiadas para el negocio y sus objetivos.

*Etapa No. 6*

**DESARROLLAR PLANES DE MEJORAMIENTO.**

- En ésta etapa se revisan los problemas inmediatos a fin de determinar acciones correctivas e implantarlas en el corto plazo con el fin de estabilizar los Sistemas de Información actuales.

## IV.3 *CONCLUSIÓN DEL ESTUDIO.*

Como resultado del estudio realizado a las anteriores metodologías, obtuvimos un panorama que nos proporcionó elementos valiosos para tomar cursos de acción, mismos que a nuestro juicio nos ayudaron a elegir de cada una de las metodologías algunos de los aspectos que ahora forman parte de una guía práctica para el desarrollo de auditorías en Informática, reconocemos de antemano que no se trata de encontrar el hilo negro, puesto que ya existen diferentes metodologías, sin embargo quisimos realizar una guía que nos llevara de la mano paso a paso.

***Primera metodología:***

Como nos podemos dar cuenta, ésta es una metodología muy completa que conforme la vamos analizando, podemos ver que cuenta con todos los elementos que necesitamos para realizar Auditorías en Informática , esto lo podemos constatar ya que la mayoría de los autores que han hecho nuevas metodologías para el desarrollo y aplicación de Auditorías en Informática o temas relacionados, han consultado ésta metodología, incluso han tomado partes de ella para complementar las propias; al igual que ellos, hemos adoptado pasos y tareas de ésta metodología , con algunas modificaciones que se adecuen a nuestros requerimientos.

*Segunda metodología.*

Al revisar ésta metodología, nos pareció que sería de gran ayuda para complementar nuestra guía, ya que nos proporciona claramente los diferentes tipos de controles que se deben evaluar para que los sistemas de información funcionen adecuadamente, y podemos identificar la existencia y funcionalidad de mecanismos de control sobre las áreas de Informática.

Esta metodología nos permitirá crear un procedimiento que nos ayude a evaluar dichas áreas, realizando algunas actividades que nos permitan complementar las tareas correspondientes.

*Tercera metodología*

Como podemos ver ésta metodología es el lado opuesto de la primera ya que no contiene los elementos básicos que se requieren para llevar a cabo un proceso metodológico. Es por eso que decidimos ponerla en este estudio como un ejemplo representativo de las diferentes metodologías existentes y hacer una comparación.

Demás está mencionar que de ésta metodología casi no elegimos elementos para llevar a cabo nuestro proyecto. Con esto no estamos criticando el trabajo de Mancera S.C, sino simplemente estamos señalando la problemática que nos encontramos al tratar de elegir elementos que nos ayuden a desarrollar nuestro propio proceso metodológico.

El desarrollo de la ***guía práctica para la aplicación de Auditorías en Informática*** la cual presentamos en el **capítulo V.**

# CAPÍTULO V

# GUÍA PRÁCTICA PARA LA APLICACIÓN DE AUDITORÍAS EN INFORMÁTICA.

## V.1 Estrategia utilizada como base para el desarrollo de la Guía práctica para la aplicación de Auditorías en Informática.

La guía que nosotros proponemos en el presente capítulo está basada en el siguiente esquema estratégico para implantar un proceso metodológico bajo un esquema práctico.

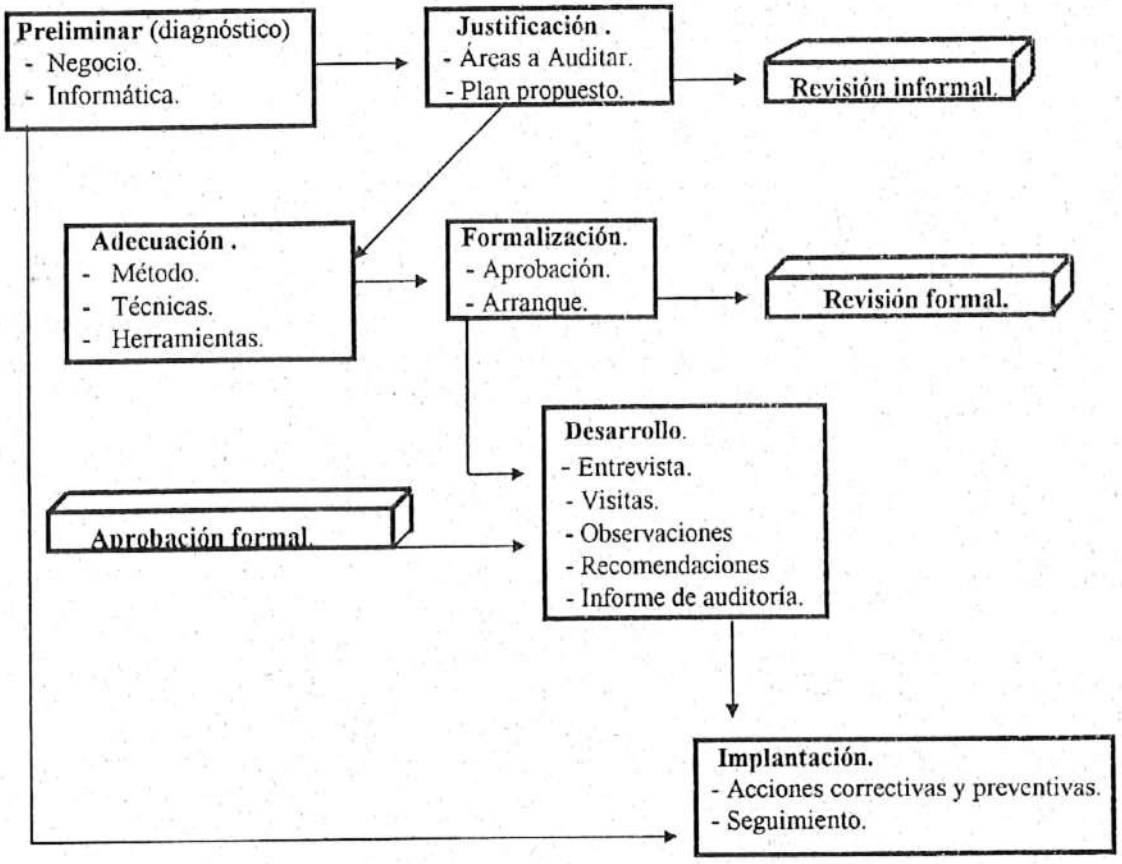


**Fig. V.1.** Estrategia para implantar un proceso metodológico de Auditoría en Informática. (Enfoque práctico).

## V.2 *GUÍA PRÁCTICA PARA EL DESARROLLO DE AUDITORÍAS EN INFORMÁTICA.*

El desarrollo de esta guía, está basado en un estudio realizado a diferentes Metodologías para el desarrollo de Auditorías en Informática , de bibliografía sobre Auditoría en Informática y áreas afines.

### *PRIMERA ETAPA.*

*FASE: **Actividades de la propuesta de una Auditoría en Informática***

TAREAS:

1.- Identifique una institución donde realizar su Auditoría en Informática, y realice un convenio hablado con los directivos .

2.- No olvide plantear claramente el significado de Auditoría en Informática, actividades a realizar y alcance de la misma.

3.- Solicite una entrevista inicial para realizar su investigación preliminar, la cual busca definir claramente áreas de análisis, responsabilidades por parte de cada participante, así como tiempos y costos estimados .

### *SEGUNDA ETAPA:*

*FASE: **Investigación Preliminar.***

TAREAS:

1.- Obtenga información sobre el ambiente macro de la empresa a través de fuentes externas (publicidad, folletería, preguntas informales a conocidos etc.).

2.- Realice su primer entrevista con el directivo de mayor jerarquía posible, en la cual deberá obtener información específica de la empresa.

3.- Realice su segunda entrevista con el Director de informática y solicite información relacionada con el departamento de informática.

4.- Realice su recorrido por las instalaciones de la empresa.

5.- Defina áreas a Auditar, haciendo una estimación del personal necesario y tiempo, todo esto es en base al " Análisis Preliminar" que usted ya realizó en las anteriores tareas.

***TERCERA ETAPA.***

*FASE:* ***Análisis de las Áreas a Auditar.***

TAREAS.

1.- ***Áreas:*** Departamento de Informática, Software, Hardware e Información.

2.- Se debe abordar cada área por separado aún cuando alguna información sea útil para varias áreas.

3.- Primeramente se deben detectar los ***RIESGOS FACTIBLES*** en el área en cuestión, se debe apoyar en riesgos genéricos y determinar riesgos específicos.

4.- Posteriormente se deben de listar una serie de ***PROBLEMAS*** que puedan materializar dichos riesgos.

5.- Una vez con los problemas es mas fácil definir ***CONTROLES FACTIBLES*** para contrarrestar cada uno de los riesgos detectados, es importante diseñar una ***" MATRIZ DE RIESGO CONTROL"***

6.- Realizar los pasos definidos en la "Metodología", de la "Propuesta de Servicios de Auditoría en Informática".

7.- Al realizar los pasos de la " Metodología", se buscará validar la probabilidad de ocurrencia de los ***RIESGOS FACTIBLES***, así como, detectar algunos no tomados en cuenta.

8.- Al realizar los pasos de la "Metodología", se buscará también, Verificar la existencia de los ***CONTROLES*** propuestos, así como, registrar los controles en uso no propuestos.

*CUARTA ETAPA.*

*FASE:* ***Informe Final.***

TAREAS:

1.- Interpretar la información obtenida para cada área analizada.

2.- Elaborar el reporte final.

3.- Hacer entrega al personal indicado el resultado del análisis.

### V.1.1 Aprobación formal de los puntos.

Se recomienda que en cada fase hay que aprobar una tarea para avanzar a la siguiente.

Se debe de estar de acuerdo en:

- Terminar una tarea.
- Efectuar modificaciones a las tareas.

## DESARROLLO DE LA GUÍA PRÁCTICA.

*PRIMERA ETAPA.*

*FASE : **Actividades de la propuesta de una Auditoría en Informática.***

*DESARROLLO DE LAS TAREAS.*

*1.- **Identifique una institución donde realizar su Auditoría en Informática o reciba la solicitud de Auditoría en Informática por parte de alguna empresa, y realice un convenio hablado con los directivos en ambos casos.***

*2.- **No olvide plantear claramente el significado de Auditoría en Informática, actividades a realizar y alcance de la misma.***

Se debe dejar bien claro a los directivos el significado y las actividades a realizar de la auditoría en Informática, con la finalidad de que conozcan los beneficios que puede obtener la institución a través de ella, como son la solución de problemas, detección de ellos y dar un dictamen de la situación actual de su empresa.

El alcance de la Auditoría se definirá claramente a través de " La carta de propuesta de servicios de Auditoría en Informática " la cual se realizará una vez desarrollado el Análisis Preliminar.

***3.- Solicite una entrevista inicial para realizar su investigación preliminar, la cual busca definir claramente las áreas de análisis, responsabilidades por parte de cada participante, así como tiempos y costos estimados.***

*SEGUNDA ETAPA:*

*FASE: INVESTIGACIÓN PRELIMINAR.*

La investigación preliminar es el primer paso práctico del Auditor en Informática dentro de las empresas o instituciones al efectuar un proyecto de Auditoría en informática. En esta etapa se debe recopilar información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitudes de documentos, la finalidad es definir el objetivo y el alcance del estudio así como el programa detallado de la investigación.

El éxito de esta etapa depende de seguir los siguientes pasos:

- Estudiar hechos y no opiniones.
- Investigar las causas, no los efectos.
- Atender razones no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y datos recabados.

Es conveniente aclarar que no se debe tratar esta etapa como un conjunto de tareas que requieren muchos recursos involucrados ni un tiempo considerable; es simplemente un aspecto necesario y generalizado para entender los puntos débiles y fuertes de la función de informática.

*Antes de iniciar la etapa del análisis preliminar se debe considerar las siguientes técnicas para la recopilación de información.*

*Como obtener información:*

1.- Se recomienda obtener información a través de 4 medios de recopilación: Visual, encuestas, entrevistas, y documentos.

2.- El Auditor deberá utilizar el medio más adecuado de acuerdo a la información que requiera, pudiendo combinar varios de ellos.

3.- Se recomienda planear detalladamente la recopilación de información antes de llevarlo a cabo.

***Recopilación de información:***

***Visual.***

- Se deben definir los aspectos a observar en cada visita a la institución.
- Su registro debe ser mental.

***Encuestas.***

- Se recomienda realizar encuestas cuando se requiera la misma información de un número alto de personas.
- Se deben realizar preguntas concretas y claras.
- Se recomienda utilizar preguntas de opción múltiple.
- La persona que realiza la encuesta debe saber correctamente el significado de cada pregunta.

***Entrevistas.***

- Se utilizan entrevistas para obtener información estimativa del personal.
- Se recomienda realizar entrevistas cortas.
- No se deben solicitar muchas entrevistas a la misma persona.
- La persona que realiza la encuesta debe saber correctamente el significado de cada pregunta.

***Documentos.***

- Se deben solicitar documentos sobre información muy precisa en la empresa.
- Debe verificarse la vigencia de los documentos solicitados.
- Se deben obtener copias de los documentos originales.

☛ Para llevar a cabo la recopilación de la información en las diferentes etapas de la guía, proporcionamos algunas herramientas en el **ANEXO A,** las cuales podrán ser modificadas de acuerdo a la actividad empresarial en la que se realizará la Auditoría y de acuerdo al criterio y necesidades del Auditor.

*DESARROLLO DE TAREAS*:

Inicio del análisis preliminar:

*1.- Obtenga información sobre el ambiente Macro de la empresa a través de fuentes externas (publicidad, folletería, preguntas informales a conocidos etc.).*

- Esta tarea consiste en obtener un panorama de la situación actual de la empresa o institución a auditar a partir del ambiente externo que rodea la empresa.

*2.- Realice su primer entrevista con el directivo de mayor jerarquía posible, en la cual deberá obtener información específica de la empresa.*

La información que se debe de obtener en la primera entrevista es la siguiente:

- Historia de la institución.
- Personal que labora en la empresa.
- Políticas generales.
- Objetivos a corto mediano y largo plazo.
- Organigrama de la empresa.
- Opinión sobre su posición en el sector.
- Procure obtener información escrita.
- Solicite una entrevista con el Director de Informática.
- Solicite un recorrido por las instalaciones de la empresa, para que lo presenten ante el personal, solicite que lo presenten como " Asesor de uso eficiente de equipo de cómputo" por ejemplo.
- Solicite una reunión para la presentación de la " propuesta de servicios de Auditoría en Informática".

*3.- Realice su segunda entrevista con el Director de informática y solicite información como la siguiente:*

- Personal que labora en el departamento.
- Políticas del departamento.
- Objetivos a corto, mediano y largo plazo del departamento.
- Organigrama del departamento.
- Opinión sobre la situación de la empresa.
- Situación presupuestal de su departamento.
- Procure obtener información escrita.
- Solicite que lo acompañe en el recorrido por la empresa.

*4.- Realice su recorrido por las instalaciones de la empresa.*

Tomando en cuenta lo siguiente:

- Procure ir acompañado por personas de rangos altos de la empresa.
- Observe y cuestione sobre el equipo de cómputo existente, preguntas sobre proveedores, tiempo de adquisición, utilidad, redes, entre otras cosas.
- Observe y cuestione sobre el manejo de información aspectos como, la cantidad de papeles que fluyen en la empresa, o que están sobre los escritorios, la forma en que se transfiere la información entre personal y departamentos, entre otras cosas.
- Observe y cuestione sobre los sistemas de cómputo utilizados, pregunte sobre amigabilidad, facilidad de uso, consistentes, entre otros.
- Procure hacer preguntas tanto a sus acompañantes como a los usuarios, intente hacer comentarios agradables sobre lo positivo que observe, principalmente a los usuarios. Lo que detecte en mal funcionamiento, sólo trate de anotarlo en su memoria.

*5.- Defina áreas a Auditar, haciendo una estimación del personal necesario y tiempo, todo esto es basándose en el " Análisis Preliminar" que usted ya realizó, se puede basar en lo siguiente:*

- Basarse en la " Técnica de Planeación de Auditoría en Informática" para definir las áreas a Auditar. ☛ Ver **anexo B**
- Basándose en el tamaño de la empresa, la cantidad de sistemas y equipo detectado, proponga un tiempo y personal estimado.
- Elabore la " Propuesta de servicios de Auditoría en Informática ".

Para desarrollar esta tarea se presenta ejemplo en: ☛ el **ANEXO C.**

- Haga la presentación de la "Propuesta de Servicios de Auditoría en Informática" y aclare puntos descritos en la propuesta, así como, modificaciones a la misma.

- Defina fecha de entrega de "Contrato de Auditoría en Informática" y fecha de reunión para firmar dicho contrato.

  Para realizar correctamente esta tarea se propone un formato preestablecido en:

  ☛ el **ANEXO D.**

*TERCERA ETAPA.*

*FASE: ANÁLISIS DE LAS ÁREAS A AUDITAR.*

*DESARROLLO DE TAREAS.*

1.- ***Áreas a Auditar:***

- Departamento de informática
- Software
- Hardware
- Información.

2.- Se debe abordar cada área por separado aún cuando alguna información será útil para varias áreas.

3.- Primeramente se deben detectar los ***RIESGOS FACTIBLES*** en el área en cuestión, se debe apoyar en riesgos genéricos y determinar riesgos específicos.

Posteriormente se deben de listar una serie de ***PROBLEMAS*** que puedan materializar dichos riesgos.

Una vez con los problemas es mas fácil definir ***CONTROLES FACTIBLES*** para contrarrestar cada uno de los riesgos detectados.

Para desarrollar las tres tareas anteriores se presenta el siguiente ejemplo:

*ANÁLISIS DEL DEPARTAMENTO DE INFORMÁTICA*

**Riesgos factibles:**

1.- Incumplimiento de los objetivos de la organización por parte del departamento de Informática.

2.- Mal funcionamiento del departamento de Informática.

3.- Mal funcionamiento del personal del departamento de Informática.

**Problemas factibles:**

*1.- Incumplimiento de los objetivos de la Organización por parte del departamento de Informática.*

- Objetivos no definidos o mal definidos.
- Objetivos del departamento incongruentes con los de la Organización.
- Incumplimiento de los objetivos por parte del personal del departamento.
- Otros.

*2.- Mal funcionamiento del departamento de Informática.*

- Políticas del departamento no definidas o mal definidas.
- Incumplimiento de las políticas del departamento.
- Conocimientos inadecuados del personal del departamento.
- Recursos escasos para realizar las tareas del departamento.
- Otros.

*3.- Mal funcionamiento del personal del departamento de Informática.*

- Mala motivación al personal.
- Descontrol en la asignación de tareas.
- Exceso de tareas y responsabilidades.
- Falta de capacitación.
- Otros.

***Controles factibles:***

***1.- Incumplimiento de los objetivos de la Organización por parte del departamento de Informática.***

- El Director de Informática definirá los objetivos del departamento en base a los de la Organización.
- El Director de Informática validará y difundirá constantemente los objetivos del departamento.
- Otros.

***2.- Mal funcionamiento del departamento de Informática.***

- Definir políticas del departamento y monitorear su cumplimiento.
- Definir políticas de selección de personal, brindarles capacitación adecuada y constante.
- Control anual de gastos, para definir presupuestos confiables.
- Otros.

***3.- Mal funcionamiento del personal del departamento de Informática.***

- Definir acciones de motivación económicas y de reconocimiento.
- Definir políticas de asignación de tareas y responsabilidades.
- Monitorear avances de tareas.
- Otros.

***Planeación de la recopilación de información:***

Por cada control detectado en los riesgos ya definidos, identificar la pregunta necesaria para obtener información sobre su existencia, así como, el medio adecuado. Por ejemplo:

**Problemas/Controles.**

***1.- Incumplimiento de los objetivos de la organización por parte del departamento de Informática.***

- El Director de Informática definirá los objetivos del departamento basándose en los de la organización.
- El Director de Informática validará y difundirá constantemente los objetivos del departamento.

**Preguntas:**

***El Director de Informática definirá los objetivos del departamento en base a los de la organización.***

1.- Obtener los objetivos de la empresa. (Documento).

2.- Obtener los objetivos del departamento. (Documento)

***El Director de Informática validará y difundirá constantemente los objetivos del departamento.***

1.- Pedir al personal que describa los objetivos principales de la empresa y del departamento. (Encuesta).

2.- Pregunta al directivo de Informática como se difunden los objetivos de la empresa y del departamento. (Entrevista).

3.- Pregunta al directivo de Informática como se monitorea el cumplimiento de objetivos. (Entrevista).

4.- Realizar los pasos definidos en la "Metodología", de la "Propuesta de Servicios de Auditoría en Informática".

5.- Al realizar los pasos de la " Metodología", se buscará validar la probabilidad de ocurrencia de los ***RIESGOS FACTIBLES***, así como, detectar algunos no tomados en cuenta.

6.- Al realizar los pasos de la "Metodología", se buscara también, Verificar la existencia de los *CONTROLES* propuestos, así como, registrar los controles en uso no propuestos.

Esta tarea es realizada basándose en la información recopilada anteriormente.

*CUARTA ETAPA.*

*FASE: INFORME FINAL.*

*DESARROLLO DE TAREAS.*

***1.- Interpretar la información obtenida para cada área analizada.***

***Se realiza el análisis de la información obtenida la cual consiste en seguir los siguientes pasos:***

- Argumentos del análisis.
- Riesgos factibles y su evaluación
- Controles recomendados.
- Definir políticas de seguimiento de uso de controles.
- Informe ejecutivo de Auditoría en Informática.

Para llevar a cabo cada uno de los pasos anteriores a continuación se presentan los siguientes ejemplos respectivos para ilustrar su desarrollo.

## *EJEMPLO DEL ANÁLISIS DEL DEPARTAMENTO DE INFORMÁTICA*

***1.- Argumentos del análisis:***

Explicar porque es clasificado cada control en la categoría descrita, *describiéndolos en el orden en que se presentan en su respectiva tabla, por ejemplo:*

- ***Dar a conocer los objetivos de la organización y del departamento de Informática.***

1.- El personal de Informática no conoce los objetivos de la empresa.

2.- El personal de Informática no conoce los objetivos de Informática.

3.- El personal de Informática menciona objetivos distintos.

### 2. *Riesgos factibles y su evaluación.*

Para cada riesgo de cada sub área listar los controles que los pueden contrarrestar, ordenándolos de mayor a menor importancia, y diga la forma en que son actualmente utilizados, por ejemplo:

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Incumplimiento de objetivos de la Organización por parte del depto. de Informática. | Dar a conocer adecuadamente los objetivos de la Organización al personal del departamento de Informática. | | ✓ | | | |
| | Objetivos del departamento congruentes con los de la organización. | | | | ✓ | |
| | Monitoreo del cumplimiento de los objetivos por parte del personal del departamento. | | ✓ | | | |
| b)Incumplimiento de los objetivos del departamento de Informática. | El Director de Informática definirá los objetivos del departamento de Informática en base a los de la Organización en general. | | | | ✓ | |
| | El Director de Informática difundirá y validara constantemente los objetivos del departamento. | | ✓ | | | |

N = nunca D= deficiente A = aceptable G = generalmente S = siempre.

**Tabla V.1** Riesgos factibles y su evaluación (ejemplo).

### 3.- *Controles recomendados:*

Basándose en el análisis anterior determinar cuáles de los controles existentes permanecerán, y determinar cuáles de los no existentes serán recomendados para mejorar la seguridad en el salvaguardo de los recursos de Información, por ejemplo:

***Controles recomendados***

***Área de:*** Departamento de Informática.

***Sub área:*** Organización del área

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Incumplimiento de objetivos de la organización por parte del depto. de Informática. | Dar a conocer adecuadamente los objetivos de la Organización al personal del departamento de Informática. | | ☑ |
| | Objetivos del departamento congruentes con los de la Organización. | ☑ | |
| | Monitoreo del cumplimiento de los objetivos por parte del personal del departamento. | | ☑ |

**Tabla V.2** Controles recomendados. (ejemplo).

*4.- Definir políticas de seguimiento de uso de controles.*

De cada uno de los controles recomendados y aceptados se deberá definir una serie de acciones que puedan ayudar a mantenerlos vigentes, para esto se recomienda definir los siguientes cuestionamientos:

| *Preguntas* | *Finalidad que determinan* |
|---|---|
| ¿ Qué? | El propósito |
| ¿ Dónde? | El lugar |
| ¿ Cuándo? | El orden y el momento (sucesión) |
| ¿ Quién? | La persona responsable |
| ¿ Cómo? | Los medios |
| ¿ Cuánto? | La cantidad |

Para definir las respuestas de las cuestiones anteriores para cada control propuesto, o inclusive para evaluar los controles ya existentes, estos pueden ser sometidos a una nueva pregunta, la cual planteará un nuevo examen que habrá de justificar la información obtenida. Cada interrogante se debe descomponer de la siguiente manera:

1.- Propósito.

a).- ¿ Qué se hace?

b).- ¿ Por qué se hace?

c).- ¿ Qué otra cosa podría hacerse?

d).- ¿ Qué debería hacerse?

2.- Lugar.

a).- ¿ Dónde se hace?

b).- ¿ Por qué se hace ahí?

c).- ¿ En qué otro lugar podría hacerse?

d).- ¿ Dónde debería hacerse?

3.- Sucesión.

a).- ¿ Qué se hace?

b).- ¿ Por qué se hace entonces?

c).- ¿ Cuándo podría hacerse?

d).- ¿ Cuándo deberá hacerse?

4.- Persona.

a).- ¿ Quién lo hace?

b).- ¿ Por qué lo hace esa persona?

c).- ¿ Qué otra persona podría hacerlo?

d).- ¿Quién debería hacerlo?

5.- Medios.

a).- ¿ Cómo se hace?

b).- ¿ Por qué se hace de ese modo?

c).- ¿ De qué otro modo podría hacerse?

d).- ¿ Cómo debería hacerse?

6.- Cantidad.

a).- ¿ Cuánto se hace?

b).- ¿ Por qué se hace esa cantidad (volumen)?

c).- ¿ Cuánto podría hacerse?

d).- ¿ Cuánto debería hacerse?

***Ejemplo*** : *Definición de políticas de seguimiento de uso de controles, del área de equipos de cómputo (Hardware)*

- **Definir políticas de adquisición y rendimiento de los equipos.**

**1.- Propósito:**
Se deben de definir políticas de adquisición y rendimiento de los equipos con el propósito de no cometer errores al hacer las adquisiciones .

**2.- Lugar:**
En el departamento de informática .

**3.- Sucesión:**
Cada que sea necesario implantar, modificar o eliminar políticas de adquisición.

**4.- Persona:**
El Director de informática en conjunto con el jefe de compras de la organización.

**5.- Medios:**
A través de juntas con los directivos de la organización y con los jefes de los departamento involucrados (compras)en la adquisición de los equipos.

**6.- Cantidad:**
Las políticas que sean necesarias.

***2.- Elaborar el reporte final o informe ejecutivo de Auditoría en Informática.***

Como resultado del trabajo de la evaluación del auditor, se debe presentar a la dirección una opinión profesional, que presente la situación de la organización.

La presentación de un informe puede hacerse de la siguiente manera:

1.- Una breve descripción de la situación actual en la cual se reflejen los puntos más importantes.

Este informe se presenta a la dirección.

2.- Una descripción detallada que comprende:

a). Los problemas detectados.

b). Posibles causas, problemas y fallas que originaron la situación presentada.

c). Efectos que pueden tener los problemas detectados.

d). Alternativas de solución.

f). Si se opta por alguna alternativa de solución, cuales son sus efectos, ventajas y desventajas así como el tiempo estimado para efectuar el cambio.

3.- Se debe hacer hincapié en como se corregirá el problema o se mejorará una determinada situación, como se obtendrán los beneficios, en cuanto tiempo y cuales son sus puntos débiles.

4.- Se debe romper la resistencia a la lectura que tienen algunos ejecutivos, por medio de conclusiones concretas que sean sencillas.

***3.- Hacer entrega al personal indicado el resultado del análisis.***

El personal indicado son:

- *El Director General de la Organización.*
- *El Director del Departamento de Informática.*

Para llevar acabo esta tarea del informe final desglosado, se propone el siguiente formato:

| *Informe Final de Auditoría en Informática.*<br>**Dirección:** _____<br>**Auditoría a:** _____<br>**Hoja No. De** |
|---|
| **Problemática:** |
| **Causas :** |
| **Consecuencias :** |
| **Alternativas de Solución:** |
| **Observaciones:** |

**Tabla V.3** Informe final de la Auditoría en Informática desglosado. ( Ejemplo).

# CAPÍTULO VI

# DESARROLLO DEL CASO PRÁCTICO

En este capítulo se implantará la guía práctica para la aplicación de Auditorías en Informática propuesta en el **CAPÍTULO V.**

## VI. 1 Desarrollo del caso práctico.

El desarrollo del caso práctico se realizará siguiendo cada una de las etapas de la guía en la aplicación de una Auditoría en Informática.

**Desarrollo de la primera etapa:**

*FASE: Actividades de la propuesta de una Auditoría en Informática*

- ***Identificación de la Institución:***

La Auditoría se aplicará en el centro de cómputo de la Comisión Estatal de Servicios Públicos de Ensenada (C.E.S.P.E.), siendo ésta una Institución que tiene como función el cumplimiento y realización de los sistemas de agua potable y alcantarillado de agua negras de cada uno de los municipios a que corresponden.

El convenio de la Auditoría lo realizamos con el Coordinador del Departamento de Informática Lic. Alfonso Talavera Hernández.

**Desarrollo de la segunda etapa.**

*Fase:* ***Investigación Preliminar.***

- ***Información sobre el ambiente macro de la empresa.***

La Comisión Estatal de Servicios Públicos de Ensenada (C.E.S.P.E.) es una institución gubernamental que se relaciona con diferentes Organismos como lo son:

- La Administración Pública del Estado.
- Comisión Federal de Electricidad.
- Ayuntamientos.
- Secretaría de Ecología y Protección al medio ambiente.
- Catastro Municipal.
- Secretaría de Hacienda y Crédito Público.
- ISSSTECALI.

- ***Información obtenida a través de la primer entrevista con el Director de Informática.***

**Historia del Organismo.**

El primer dato respecto a la infraestructura hidráulica en el municipio de Ensenada, se refiere a la red de agua potable que iba de la calle Ryerson a la Av. Gastélum y de la calle Frente a la calle 14ª. El agua que suministraba ésta red se demandaba de un tanque de almacenamiento que se encuentra arriba de la calle 6ta. entre la calle Ryerson y calle 20 de Noviembre.

Mucho después dado el crecimiento del Municipio de Ensenada, y de las necesidades de la Población que lo componían, se formó el departamento de agua, dependiente del departamento de Obras Públicas Municipales, responsabilizando al Ing. René Barrera Villavicencio de esa unidad Administrativa de nueva creación.

El departamento de agua funcionó como tal, hasta el 31 de Agosto de 1968, fecha en que entró en vigor el Derecho No.139 que le otorga el carácter de Organismo Público de Ensenada.

El nuevo Organismo empezó a operar el 1ro. de Diciembre de 1968 en Av. Ruiz No.36 zona centro designando al Ing. Luis de Basave López Portillo como Gerente General del mismo, el Ing. Basave en nombre de su representada solicitó un crédito de $ 25,000,000.00 (Veinticinco millones de pesos) de ese entonces como apoyo al inicio de operaciones y cumplimiento a las necesidades inmediatas que ya como organismo tenía que cumplir, mismo que se le otorgó por conducto de BANOBRAS a un plazo de 20 años.

La Comisión Estatal de Servicios Públicos de Ensenada, para ese entonces estaba conformada con una plantilla de personal de alrededor de 48 personas cuyo gasto por concepto de nómina mensual aproximadamente correspondía a $ 65,000.00 (Sesenta y cinco mil pesos de ese entonces) y se distribuía en una estructura Orgánica que correspondía al consejo de Administración, Auditor externo y Secretario de consejo, a un Gerente General, Auditor interno, Asesor legal y Secretaría, apoyándose por dos gerencias cuyas actividades se centraban en Administración y técnica.

Ésta estructura se mantuvo de la misma forma sólo sufriendo cambios de Organización en las áreas operativas exclusivamente de la Administración del Ing. Humberto Noble Granados, período comprendido de Noviembre de 1971 a Noviembre de 1977.

Al concluir la Administración del Ing. Noble Granados, la atención que este Organismo brindaba en cuanto al número de tomas domiciliarias era de 13,439 aunándole la infraestructura hidráulica que ya se poseía.

Durante la Administración del Ing. Carlos Mcfarland Corona se dieron cambios importantes en el rubro de la normatividad que regulaba al Organismo, ya que en fecha 10 de Febrero de 1979, por encargo de despacho por Ministerio de Ley en C. Secretario General de Gobierno, manda publicar la Ley de las Comisiones Estatales de Servicios Públicos, reflejando con esto aún más la autonomía que como Organismo descentralizado se tiene y plasmado el mandato social de acercamiento de las instancias de Gobierno en los Municipios de nuestro Estado.

Con lo anteriormente señalado el Organismo vio modificado su Organización elevando Administrativamente de Gerencia General y Gerencias a Dirección General y Direcciones respectivamente.

Durante la Dirección del Ing. Carlos Loyola Peterson, la C.E.S.P.E. dio muestras de entereza y determinación a lo largo de su creación, y en años recientes fue sorteando los problemas que le son particulares y cumpliendo con su parte en la solución de aquellos que incumben a todos los Ensenadenses.

Actualmente, el Director General de la C.E.S.P.E. es Marco Antonio Carrillo Robles.

- ***Personal que labora en la empresa.***

| PERSONAL DE BASE | PERSONAL DE CONFIANZA | PERSONAL TEMPORAL |
|---|---|---|
| 1. Jefe de sección E | Director General | Recaudador Auxiliar |
| 2. Jefe de sección D | Coordinador de Planeación | Operador Maquinaria |
| 3. Jefe de sección C | Subdirector Administrativo | Encargado de Departamento |
| 4. Jefe de sección B | Subdirector Comercial | Auxiliar Recaudación |
| 5. Jefe de sección A | Subdirector Técnico | Auxiliar Operación y Manto. |
| 6. Subjefe de sección | Subrecaudador adscrito | Auxiliar Administrativo |
| 7. Oficial Administrativo AA | Coord.de Obras y Proyectos | Auxiliar Almacén |
| 8. Inspector | Coord. De Sistemas foráneos | Auxiliar servicios Generales |
| 9. Químico | Coordinador Comercial | Auxiliar Supervisor |
| 10. Oficial Administrativo A | Coordinador Financiero | Plomero |
| 11. Jefe de Brigada | Coordinador Informática | Velador |
| 12. Oficial Administrativo | Jefe de departamento | Peón |
| 13. Sobrestante B | Encargado de departamento | |
| 14. Operador de máquinas | Supervisor | |
| 15. Plomero | Auditor interno | |
| 16. Sobrestante A | Residente | |
| 17. Topógrafo | Cajeras | |
| 18. Mecánico automotriz | Analista | |
| 19. Mecánico medidores | Programador | |
| 20. Técnico electricista | Dibujante | |
| 21. Notificador | Auxiliar Administrativo | |
| 22. Auxiliar de Almacén | Promotor de Obras | |
| 23. Aux.Op.maquinaria | Notificador | |
| 24. Chofer | Recepcionista | |
| 25. Ejecutor | Electricista | |
| 26. Lecturista | Secretaria | |
| 27. Oficial Administrativo C | Velador | |
| 28. Oficial de mantenimiento | Vigilante | |
| 29. Albañil | Auxiliar vigilante | |
| 30. Bombero | Peón | |
| 31. Compresorista | | |
| 32. Auxiliar mecánico | | |
| 33. Auxiliar laboratorio | | |
| 34. Auxiliar Administrativo | | |
| 35. Auxiliar Plomero | | |
| 36. Auxiliar topógrafo | | |
| 37. Ayudante perforista | | |
| 38. Ayudante oficial A | | |
| 39. Ayudante electricista | | |
| 40. Vigilante | | |
| 41. Peón | | |

**Tabla VI.1** Personal que labora en la empresa.

- ***Políticas generales.***

Las políticas generales de la Organización no están documentadas (manual de políticas), sin embargo se formalizan a través de oficios y memorándums.

- ***Objetivos a corto, mediano y largo plazo.***

El objetivo principal de la Institución es suministrar agua potable a todo el municipio de Ensenada B.C., tratando de cumplir siempre con las actividades que promuevan los principios de probidad, eficiencia, vigilancia y control, todos estos inmersos dentro de una planeación proyectada en la sistematización de tareas, retribución de responsabilidades y vinculación adecuada de esfuerzos encaminados a reducir las diferencias en el desarrollo de los objetivos Institucionales del Organismo.

- ***Organigrama de la empresa.***

(Ver página adjunta)

- ***Opinión sobre su posición en el sector.***

" Siendo una institución gubernamental que no tiene competencia alguna en el sector, ha dado muestras de entereza y determinación a lo largo de su creación; y en años recientes ha ido sorteando los problemas que le son particulares y cumpliendo con su parte en la solución de aquellos que incumben a todos los Ensenadenses."

## ORGANIGRAMA DE LA COMISIÓN ESTATAL DE SERVICIOS PÚBLICOS DE ENSENADA.

## ESTRUCTURA ORGÁNICA 1996.

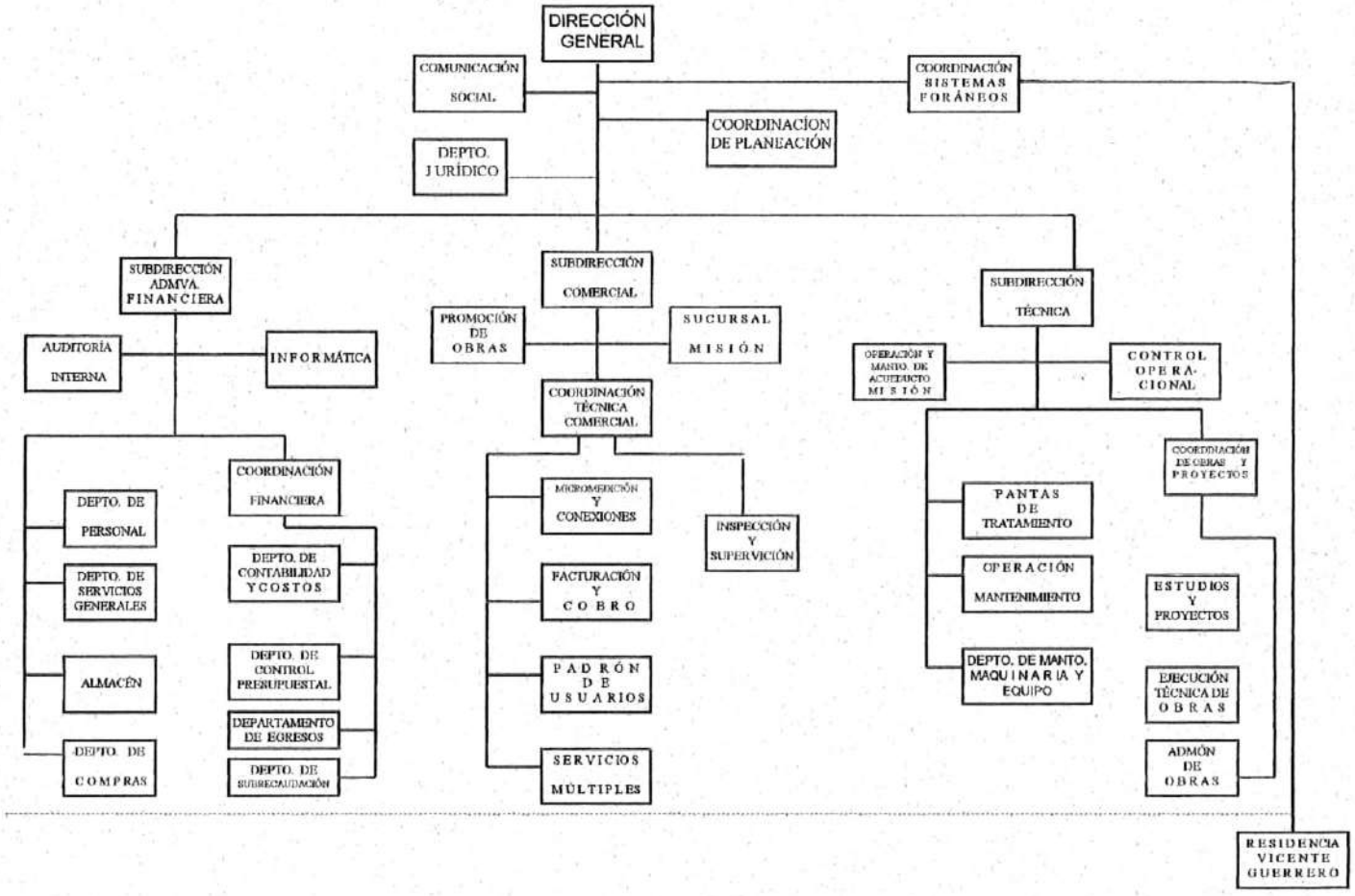


**Figura VI.1** Estructura Orgánica de la Comisión Estatal de Servicios Públicos de Ensenada.

***Información obtenida de la entrevista realizada al Director de Informática:***

- ***Personal que labora en el departamento.***

El total de personas que labora en el área de Informática es de 8 personas:

- 1 Coordinador
- 2 Analistas programadores
- 1 Encargado de mantenimiento y equipo
- 3 Programadores
- 1 Documentador de sistemas.

- ***Políticas del departamento.***

Las políticas del departamento de Informática no se encuentran establecidas en documento formal, se dan a conocer por medio de oficios y memorándums, las cuales son:

- Respetar las líneas de sub-estación eléctrica para los aparatos de cómputo.
- Todo trabajo debe de estar respaldado por el departamento de Informática.
- Debe de encontrarse restringido el acceso al personal ajeno al área de Informática.
- Toda modificación de algún sistema debe de ser respaldado por oficio, para poder tener antecedentes.

- ***Objetivos a corto, mediano y largo plazo del departamento.***

Los objetivos a corto y largo plazo de departamento de Informática son:

- Operar el sistema de modo distribuido
- Actualizar versión Oracle
- Adquirir un nuevo equipo RISK.
- Actualizar UNIX EP-IX de control data
- Integrar el sistema de presupuestos con control presupuestal y puntos de egresos como son: almacén, compras, egresos, etc.
- Implementar sistemas de MAPEO, con aplicaciones de redes de agua y drenaje.

  Éste proyecto depende de que Catastro Municipal concluya un proyecto que proporcionará la base cartográfica para la aplicación .

- ***Organigrama del departamento.***


**Figura VI.2** Organigrama del departamento de Informática de la C.E.S.P.E.

- ***Opinión sobre la situación del departamento de Informática en la empresa.***

El Director de Informática menciona que el Departamento de Informática debe de estar a un nivel staff. Cabe mencionar que ésta actual Administración le ha dado el apoyo que se requiere para que su departamento no se vea limitado.

- ***Situación presupuestal de su departamento.***

El presupuesto del departamento de Informática es asignado anualmente por lo que se tienen que ajustar a este, aunque se dan excepciones cuando se requiere en casos de extrema urgencia.

- ***Áreas a Auditar.***

La Auditoría en Informática se basa en evaluar 4 partes principales dentro de una Organización:

1.- Evaluación de departamento de Informática.

2.- Evaluación del Software.

3.- Evaluación del Hardware.

4.- Evaluación de la información.

Estas áreas a su vez están divididas en 4 sub áreas:

1.- Evaluación de departamento de Informática.

- Organización de área
- Presupuestos/gastos
- Personal de Informática
- Personal externo

2.- Evaluación del Software.

- Etapas de desarrollo
- Control de proyectos
- Monitoreo de sistemas
- Adquisición de software general

3.- Evaluación del Hardware.

- Adquisición de los equipos
- Mantenimiento
- Control de fallas
- Uso del equipo

4.- Evaluación de la información.

- Control de entradas/procesos/salidas
- Acceso a la información
- Cuidado de la información
- Calidad de la información

- ***Estimación del personal necesario y tiempo.***

| Áreas a Auditar | Sub áreas. | Tiempo Estimado (semanas) 1 2 3 4 5 6 7 | Persona responsable |
|---|---|---|---|
| • *Departamento de Informática* | • *Organización del área.* | ✓ | *Noemí Montiel H Tesista.* |
| | • *Presupuestos/Gastos.* | ✓ | |
| | • *Personal de Informática.* | ✓ | |
| | • *Personal Externo.* | ✓ | |
| • *Software* | • *Etapas de desarrollo.* | ✓ | *Sonia R. Sánchez E. Tesista.* |
| | • *Control de proyectos* | ✓ | |
| | • *Monitoreo de sistemas.* | ✓ | |
| | • *Adquisición de Software general* | ✓ ✓ | |
| • *Hardware* | • *Adquisición de equipos.* | ✓ | *Noemí Montiel H. Tesista.* |
| | • *Mantenimiento* | ✓ | |
| | • *Control de fallas.* | ✓ | |
| | • *Uso del equipo.* | ✓ | |
| • *Información* | • *Control Entradas/ Procesos /Salidas.* | ✓ | *Ramona Estrada S. Tesista.* |
| | • *Acceso a la Información.* | ✓ | |
| | • *Cuidado de la Información.* | ✓ | |
| | • *Calidad de la información* | ✓ | |

**Figura VI.3** Estimación del personal necesario, determinación del tiempo y definición de las áreas a auditar.

- *Propuesta de Auditoría en Informática ver Anexo C*

*TERCERA ETAPA.*

*FASE: ANÁLISIS DE LAS ÁREAS A AUDITAR.*

*DESARROLLO DE TAREAS.*

*Áreas a Auditar:*

- ***Departamento de Informática***

- Riesgos/ problemas/ controles.

- ***Software***

- Riesgo/problema/ controles.

- ***Hardware***

- Riesgo/ problema/controles.

- ***Información.***

  - Riesgo/problema/controles.

# EVALUACIÓN DEL DEPARTAMENTO DE INFORMÁTICA.

## 1.- Organización del Área.

**RIESGO:**

a) Incumplimiento de los objetivos del departamento de Informática.

**PROBLEMAS FACTIBLES:**

- Objetivos del departamento no definidos o mal definidos.
- Objetivos del departamento de Informática incongruentes con los de la Organización en general.
- Objetivos no difundidos.

**CONTROLES FACTIBLES:**

- El Director de Informática definirá los objetivos del departamento de Informática basándose en los de la Organización en general.
- El Director de Informática difundirá y validará constantemente los objetivos del departamento

**RIESGO:**

b) Mal funcionamiento del departamento de Informática.

**PROBLEMAS FACTIBLES:**

- Políticas del departamento no definidas o mal definidas.
- Incumplimiento de las políticas del departamento.
- Número inadecuado de personas en el departamento.
- Conocimientos inadecuados del personal del departamento.
- Escasez de recursos para la realización de las tareas de departamento.

**CONTROLES FACTIBLES:**

- Definir políticas del departamento y monitorear su cumplimiento.
- Definir políticas de selección de personal, brindarles capacitación adecuada y constante.
- Control anual de gastos, para definir presupuestos confiables.

**RIESGO:**

c) Crear una mala imagen del departamento de Informática ante los demás miembros de la Organización.

**PROBLEMAS FACTIBLES:**

- Provocar atrasos en el desarrollo de las actividades que dependen del departamento de Informática.
- Mostrar incapacidad para resolver los problemas.
- No proporcionar el soporte requerido.

**CONTROLES FACTIBLES:**

- Contar con un plan prioritario de actividades de otros departamentos dependientes del departamento de Informática.
- Responder correctamente a los requerimientos al departamento con una buena capacitación.
- Proporcionar un soporte eficaz a los departamentos que los requieran.

**RIESGO:**

d) Mala definición de Proyectos.

**PROBLEMAS FACTIBLES:**

- No tomar parte de las decisiones de la Organización.
- Tomar parte de las decisiones, sin conocimiento de los objetivos de la Organización.
- Desconocer la capacidad del departamento de Informática.

**CONTROLES FACTIBLES:**

- Hacer la ubicación correcta del departamento de Informática.
- El Director de Informática conocerá los objetivos de la Organización.
- El Director de Informática conocerá perfectamente el alcance del departamento.
- El Departamento de Informática contará con un plan bien definido de cargas de trabajo y asignación de tiempos en cada proyecto.

**2.- Presupuestos/ Gastos.**

**RIESGO:**

a) Presupuestos insuficientes.

**PROBLEMAS FACTIBLES:**

- Mala evaluación de los presupuestos.
- Mala planeación de los presupuestos.
- Errores en la formalización de los presupuestos.
- Exceso de gastos no contemplados.
- Variaciones en el medio ambiente externo.

**CONTROLES FACTIBLES:**

- El Director de Informática vigilará la realización de una buena planeación de los presupuestos y los gastos.
- Elaboración de presupuestos Flexibles.
- Crear un fondo de contingencias o revisarlo periódicamente en caso de que exista.

**RIESGO:**

b) Surgimiento de gastos imprevistos.

**PROBLEMAS FACTIBLES:**

- Incompetencia del personal encargado de los presupuestos.
- Negligencia del encargado del departamento.
- Mal manejo y administración de los presupuestos y los gastos.

**CONTROLES FACTIBLES:**

- Se proporcionará capacitación adecuada para la realización de los presupuestos.
- Manejo adecuado del recurso humano.
- El Director de Informática llevará acabo un buen manejo y administración de los presupuestos y los gastos.

**RIESGO:**

c) Presupuestos /Gastos no aprobados.

**PROBLEMAS FACTIBLES:**

- Mala evaluación de los presupuestos.
- Errores en la elaboración de los presupuestos.
- Incapacidad para la planeación de un buen presupuesto.
- Estimación errónea de los presupuestos.

**CONTROLES FACTIBLES:**

- El Director de Informática vigilará la realización de una buena planeación de los Presupuestos /gastos del departamento.
- Se evitarán los errores en la elaboración de los presupuestos.
- Se proporcionará la capacitación necesaria para la planeación, elaboración, estimación de los presupuestos y gastos.

**RIESGO:**

d) Sobrestimar el presupuesto:

**PROBLEMAS FACTIBLES:**

- Distracción de los recursos.
- Estimación errónea del presupuesto.
- Mala utilización de los recursos.

**CONTROLES FACTIBLES:**

- Mejor elaboración del presupuesto.
- Apegarse a las partidas presupuestales.
- Aplicación de técnicas confiables en la planeación del presupuesto por personal capacitado.

**3.- Personal Externo.**

**RIESGO:**

a) Resistencia a los cambios y uso de tecnología avanzada.

**PROBLEMAS FACTIBLES:**

- Desconocimiento de las funciones del departamento de Informática.
- Falta de comunicación del personal de Informática con el personal externo.
- Mal servicio de soporte técnico por parte del personal de Informática.
- Falta de programas de capacitación (Informática) al personal externo.

**CONTROLES FACTIBLES:**

- Difundir las funciones del departamento de Informática.
- Lograr comunicarse adecuadamente con el personal externo.
- Llevar a cabo programas de capacitación para proporcionar el soporte técnico que demanda el personal externo.

**RIESGO:**

b) Mal uso de los recursos de Informática.

**PROBLEMAS FACTIBLES:**

- Falta de capacitación del personal externo.
- Incapacidad del personal de Informática para capacitar al personal externo.
- Actitudes negativas del personal externo.

**CONTROLES FACTIBLES:**

- Capacitar al personal externo en el uso de los equipos y lo que podría causar daños
- Evaluar al personal de Informática en cuanto a la capacitación que le dé al personal externo.
- Monitorear al personal externo ante su trabajo.

**RIESGO:**

c) Personal externo ineficiente en su trabajo.

**PROBLEMAS FACTIBLES:**

- Falta de capacitación
- Desconocimiento de políticas y lineamientos del uso de los equipos.
- Utilización de sistemas de cómputo poco amigables.
- Mal ambiente de trabajo entre personas.
- Malas condiciones ambientales físicas en el área de trabajo.

**CONTROLES FACTIBLES:**

- Proporcionar capacitación al personal externo.
- Difusión de políticas y funciones para el uso correcto de los equipos
- Implantación de sistema con un ambiente amigable para el usuario.
- Supervisión continua al personal externo.
- Mantener en condiciones óptimas las condiciones ambientales de la Organización
- Realizar dinámicas de grupos para mejorar las relaciones entre personas.

**4.- Personal de Informática.**

**RIESGO:**

a) Mal funcionamiento del personal de Informática.

**PROBLEMAS FACTIBLES:**

**- Mal ambiente de trabajo:**

- Desintegración y mala convivencia del personal.
- Malas condiciones ambientales con respecto:
  - ¤ Espacio ¤ Iluminación ¤ Ventilación ¤ Equipo de oficina
  - ¤ Ruido ¤ Limpieza ¤ Comunicación

**- Mal Desempeño y comportamiento del personal de Informática**

- Repetición de los trabajos asignados.
- Mal manejo de la información confidencial.
- Incumplimiento de políticas y procedimientos.
- Personal que no es cooperativo.
- Falta de sugerencias del personal.

**- Malas condiciones de trabajo.**

- Inexistencia o desconocimiento del reglamento interno de trabajo.
- Conflictos de trabajo.
- Personal mal remunerado.

**- Mala organización del trabajo.**

- No detectar anticipadamente las necesidades.
- Fallas en la selección y reclutamiento de personal.

- **Mal desarrollo y motivación del personal**.
- No hacer una correcta inducción al nuevo personal.
- No recompensar económicamente al personal.
- No motivar al personal con ascensos.

- **Mala capacitación del personal**.
- Falta de identificación de las necesidades actuales y futuras de capacitación del personal.
- No contar o elaborar un plan anual para la capacitación.
- No realizar programas de capacitación para cada área.
- No verificar los resultados de las capacitaciones proporcionadas al personal.

**CONTROLES FACTIBLES:**

- **Mal ambiente de trabajo**
- Tomar medidas para proporcionar al personal un buen ambiente de trabajo tanto en la integración entre individuos como buenas condiciones ambientales.

- **Mal desempeño y comportamiento del personal de Informática**.
- Llevará a cabo una minuciosa elección del personal, utilizando técnicas eficientes
- Imponer reglas eficaces para una buena disciplina.
- Asignar responsabilidades y delimitar la autoridad.
- Control de asignación de tareas.

- **Malas condiciones de trabajo.**
- Distribución del Reglamento interno de trabajo.
- Lograr que el personal se sienta satisfecho y bien remunerado económicamente.

**- Mala organización en el trabajo.**

- Elaboración de programas para la detección anticipada de las necesidades del área.
- Llevar un buen control en el reclutamiento y selección del personal.

**- Mal desarrollo y motivación del Personal.**

- Definir programas de motivación, recompensas y ascensos para el personal.

**- Mala capacitación del personal.**

- Identificación de las necesidades actuales y futuras para capacitación del personal.
- Elaboración de programas de capacitación.
- Verificación de los resultados de las capacitaciones.

# EVALUACIÓN DEL SOFTWARE.

**1.- Control de proyectos**

**RIESGO:**

A) Pérdida de información y de tiempo a causa de errores en los sistemas.

**PROBLEMAS FACTIBLES:**

- No se realizan las pruebas necesarias antes de su implantación.
- No se valida su capacidad de operación.
- Omisión del análisis y diseño de los sistemas

**CONTROLES FACTIBLES:**

- Elaborar pruebas exhaustivas de todos los programas que intervienen en un nuevo sistema o que han sido modificados.
- Realizar análisis y diseño de los sistemas.

**RIESGO:**

B) Retraso en la presentación de reportes.

**PROBLEMAS FACTIBLES:**

- Falta de un adecuado diseño del sistema.
- Los procesos que generan los reportes son demasiados lentos.
- Sistemas complejos para generar los reportes.

**CONTROLES FACTIBLES:**

- Tener un diseño en el sistema lo más óptimo posible y estructurado.
- Contar con un acceso inmediato a los procesos que generen los reportes.

**RIESGO:**

C) Excesivo costo en el desarrollo del sistema.

**PROBLEMAS FACTIBLES:**

- Falta de un adecuado análisis costo/beneficio.
- Inadecuada utilización de los recursos destinados para el desarrollo del sistema.
- Carencia de conocimientos y/o experiencia para la elaboración de un presupuesto.

**CONTROLES FACTIBLES:**

- Elección adecuada del personal para la elaboración del presupuesto.
- Capacitación eficiente del personal.
- Evaluación y elaboración del costo/beneficio.

**RIESGO:**

D) Dificultad para realizar el mantenimiento del sistema.

**PROBLEMAS FACTIBLES:**

- Documentación inadecuada, incompleta o inexistente.
- Personal inadecuado.

**CONTROLES FACTIBLES:**

- Establecer políticas de documentación de los sistemas.
- Seleccionar personal capacitado.

**RIESGO:**

E) El programa no cumpla con los objetivos del proyecto.

**PROBLEMAS FACTIBLES:**

- Información recabada, incompleta o inadecuada (un mal análisis).
- Falta de estándares en el desarrollo, análisis y programación.
- Objetivos del proyecto pobremente definidos.

**CONTROLES FACTIBLES:**

- Definir la finalidad del sistema correctamente en la etapa del análisis.
- Elección de un buen equipo de trabajo preparado profesionalmente.
- Establecido previo de estándares a manejar en todo el ciclo de vida del sistema.
- El directivo eligirá al personal clave para proporcionar información verídica y completa.
- Tomar en cuenta todas las áreas que estarán con el sistema.

## 2.- Etapas de desarrollo del sistema

### RIESGO:

A) Elaborar un proyecto deficiente.

### PROBLEMAS FACTIBLES:

- Inadecuada comunicación entre el usuario y los programadores.
- Escaso conocimiento para desarrollar un análisis certero.
- Fricciones laborales.
- Al no respetarse los tiempos señalados por el programa, trae consigo la deficiente elaboración de los mismos y por lo tanto el diseño de los recursos.
- Falta de conocimiento de las necesidades reales del entorno laboral aunado a una deficiente comunicación entre el usuario y el programador.

### CONTROLES FACTIBLES:

- Establecer adecuados canales formales de comunicación entre los empleados de la Organización.
- Elaborar una adecuada planeación y cumplir con los tiempos señalados.
- Previamente el operario deberá conocer el funcionamiento y actividades que en forma genérica realiza la Organización.
- Contar con una adecuada distribución del trabajo, para tener una buena organización y con esto dar como resultado una armonía en el trabajo.

**RIESGO:**

B) Error en el manejo de los archivos.

**PROBLEMAS:**

- Falta de validación de los sistemas.
- Sistemas incompletos.
- Programación inadecuada.

**CONTROLES FACTIBLES:**

- Definir un programa para determinar el tipo y la frecuencia de protección de los datos de acuerdo a su naturaleza y utilización (archivos maestros, de transacciones, acumulados, históricos y otros).

**RIESGO:**

C) Incumplimiento en tiempos de entrega de los sistemas.

**PROBLEMAS FACTIBLES:**

- Inadecuada asignación de las actividades en el personal de Informática.
- Acumulación de actividades en una persona y/o todo el personal integrante del departamento de Informática .
- Falta de planeación de las actividades.

**CONTROLES FACTIBLES:**

- Elaboración e implantación de un cronograma de actividades.
- Elección de un equipo de trabajo capacitado.
- Concluir todos los sistemas requeridos por la Organización
- Elaborar una programación bien estructurada y hacerle pruebas de verificación.

**3.- Monitoreo de sistemas**

**RIESGO:**

A) Software obsoleto.

**PROBLEMAS FACTIBLES:**

- Falta de previsión de las innovaciones tecnológicas del software en el mercado así como crecimiento y/o modificación de actividades, funciones de la Organización.

**CONTROLES FACTIBLES:**

- Revisión periódica del crecimiento y desarrollo de la Organización de las necesidades del software a las mismas.

**RIESGO:**

B) Rechazo del usuario hacia el manejo de los sistemas.

**PROBLEMAS:**

- Oposición del usuario ante la innovación tecnológica en los procesos internos de la Organización.
- Desconocimiento del usuario de los beneficios que puede proporcionar la utilización de los sistemas electrónicos dentro de la Organización.
- Falta de difusión por parte de los altos funcionarios de la Organización, hacia los trabajadores que operan el software.
- Falta de una adecuada capacitación.

**CONTROLES:**

- Tener la autoridad de los altos funcionarios de la Organización para poder dar conjuntamente con Recursos Humanos los cursos de capacitación pertinentes para los cambios de actitudes y aptitudes de los usuarios ante las innovaciones.

**4.- Adquisición del software**

**RIESGO:**

A) Incompatibilidad del software adquirido con el hardware existente.

**PROBLEMAS FACTIBLES:**

- El no realizar monitoreo adecuado del software con las innovaciones que ofrece el mercado.
- El no contar con un adecuado inventario del hardware existente en la Organización.

**CONTROLES FACTIBLES:**

- Realizar una adecuada detección de necesidades y compatibilidad del software con el hardware.
- Elaborar y actualizar inventario del hardware que tenga la Organización y en el departamento de Informática.

**RIESGO:**

B) Incompatibilidad del software adquirido con el software existente.

**PROBLEMAS FACTIBLES:**

- No contar con un monitoreo adecuado del software existente con las innovaciones que ofrece el mercado.
- No contar con un adecuado inventario del software existente en la Organización.

**CONTROLES FACTIBLES:**

- Elaborar una adecuada detección de necesidades de software en los diversos departamentos de la Organización.
- Elaborar y actualizar inventario del software.

**RIESGO:**

C) Agotamiento del presupuesto antes de lo estimado.

**PROBLEMAS FACTIBLES:**

- Que exista una devaluación y no se haya considerado dentro del programa.
- Una mala planeación y distribución de los egresos.
- Dispendio de recursos.

**CONTROLES FACTIBLES:**

- Realizar un estudio de tiempo y movimientos evaluando al personal en cuanto al manejo de los recursos disponibles.
- Capacitar al personal de la importancia que tiene el no dispendio de los recursos.
- Realizar un estudio con los índices inflacionarios en los dos últimos años, para prever la devaluación de costos de la adquisición de software a futuro.
- Elaborar una adecuada planeación para la buena distribución del presupuesto.

**RIESGO:**

D) Invertir en software innecesario.

**PROBLEMAS FACTIBLES:**

- No contar con información actualizada sobre el nuevo software que existe en el mercado.
- Falta de inventario sobre el software de la Organización.
- Desconocer lo que se está solicitando al mercado.

**CONTROLES FACTIBLES:**

- Contar con el inventario actualizado del software y con esto saber que es lo necesario y adecuado para la excelente utilización en la empresa y que exista una mayor eficacia y eficiencia.
- Asignación de un responsable para que determine que software se va adquirir o se requiere dependiendo lo que exista en el mercado.
- Actualizarse de las innovaciones del software en el mercado.

**RIESGO:**

E) Invertir en software necesario y no utilizarlo.

**PROBLEMAS FACTIBLES:**

- Falta de concientización y/o capacitación del usuario y/o personal de Informática.
- Falta de personal específico para ser capacitado.

**CONTROLES:**

- Capacitar al usuario sobre el nuevo software adquirido.
- Asignación del capacitador y el personal que recibirá la capacitación.

## EVALUACIÓN DE LOS EQUIPOS.

**1.- Adquisición.**

**RIESGO:**

a) Elección errónea de los equipos (Funcionalidad - Rendimiento)

**PROBLEMAS FACTIBLES**

- Inexistencia de un buen plan de adquisición y rendimiento de los equipos que refleje las necesidades a corto y a largo plazo.
- Incompatibilidad de los equipos.
- Falta de actualización de los inventarios de los equipos.

**CONTROLES FACTIBLES** :

- Definición de políticas de adquisición y rendimiento de los equipos.
- Realización de programas de adquisición y rendimiento de los equipos.
- Revisión y actualización periódica de los inventarios de los equipos.

**RIESGO:**

b) Utilización de procedimientos erróneos en la adquisición de los equipos

**PROBLEMAS FACTIBLES**:

- No contar con garantías sobre los equipos.
- Falta de soporte por parte del proveedor.
- No contar con capacitación para el uso y configuración de os equipos.

**CONTROLES FACTIBLES**:

- Llevar a cabo concursos para la elección del proveedor correcto.

**RIESGO:**

c) Mal pronóstico del Costo - Beneficio.

**PROBLEMAS FACTIBLES:**

- Mala realización de los estudios de factibilidad económica, operativa y tecnológica en la adquisición de los equipos.

**CONTROLES FACTIBLES:**

- Realización de estudios de factibilidad económica, operativa y tecnológica para la adquisición de los equipos.

**2. Mantenimiento.**

**RIESGO :**

a) Bajo o nulo rendimiento de los equipos.

**PROBLEMAS FACTIBLES:**

- Incumplimiento del plan de mantenimiento de los equipos.
- Número de personal de mantenimiento inadecuado.

**CONTROLES FACTIBLES:**

- Poner en practica periódica el plan de mantenimiento de los equipos.
- Contar con el número adecuado de personas para el mantenimiento de los equipos.
- Personal capacitado para el mantenimiento de los equipos.

**RIESGO :**

b) Mal Mantenimiento.

**PROBLEMAS FACTIBLES:**

- Personal inadecuado para dar mantenimiento.
- Falta de soporte a los usuarios que utilizan los equipos.
- Falta de recursos para dar mantenimiento.
- Inexistencia de reportes de mantenimiento.

**CONTROLES FACTIBLES:**

- Definición de las políticas de mantenimiento de los equipos.
- Realización de registros del mantenimiento a los equipos.
- Realización de presupuestos correctos para la inversión que requiere el mantenimiento de los equipos.

**RIESGO** :

c) Mala selección de la empresa para dar mantenimiento a los equipos.

**PROBLEMAS FACTIBLES:**

- Incumplimiento del contrato realizado para dar mantenimiento o los equipos.
- Desgaste de los equipos por incumplimiento de la empresa de mantenimiento.

**CONTROLES FACTIBLES:**

- Contratación de una empresa seria y de prestigio para dar mantenimiento a los equipos
- Elaboración de un plan de contingencias para sustituir a la empresa o personas que no cumplan con su trabajo.

**3.- Control de Fallas.**

**RIESGO:**

a) Acumulación y sobrecargas de trabajo.

**PROBLEMAS FACTIBLES:**

- Incumplimiento de actividades de los usuarios de los equipos.
- Incumplimiento o inexistencia de un plan preventivo de fallas.
- Falta de un registro o reportes de las fallas.
- Atraso para la toma de decisiones inmediatas.
- Personal incapacitado para reparación de las fallas.

**CONTROLES FACTIBLES:**

- Elaboración de un plan efectivo de prevención de fallas.
- Poner en práctica el plan preventivo de fallas y monitorearlo periódicamente.
- Elaboración de reportes de las fallas.
- Capacitación al personal para reparar las fallas.
- Contar con refacciones para la reparación de las fallas.
- Difundir a los usuarios la importancia de que se trate adecuadamente a los equipos.

**RIESGO:**

b) Pérdida de tiempo del usuario.

**PROBLEMAS FACTIBLES**:

- Atrasos en la entrega de proyectos o trabajos asignados a los usuarios.
- Mala configuración de los equipos.
- Mal ajuste de las piezas.

**CONTROLES FACTIBLES:**

- Realización de cronogramas de control de fallas.
- Bitácoras de ajuste a los equipos.

**RIESGO:**

c) Pérdida de dinero para la empresa.

**PROBLEMAS FACTIBLES**:

- Desembolsos innecesarios para reparación de fallas de los equipos.

**CONTROLES FACTIBLES:**

- Realización de un buen presupuesto de gastos para el control e fallas.

**4.- Uso de los equipos.**

**RIESGO:**

a) Maltrato o trato inadecuado de los equipos.

**PROBLEMAS FACTIBLES:**

- Desconocimiento o incapacidad de los usuarios en uso de los equipos.
- Falta de restricciones de acceso en el uso de los equipos.
- Falta de vigilancia de los equipos.

**CONTROLES FACTIBLES:**

- Capacitar a los usuarios de los equipos en el uso y funcionamiento.
- Restringir el acceso a los equipos de personal ajeno a ellos.
- Contar con vigilancia a los equipos.

**RIESGO:**

b) Maltrato o desgaste por el ambiente.

**PROBLEMAS FACTIBLES:**

- Mala distribución y ubicación de los equipos.
- Malas condiciones del centro de cómputo.
- Contar con malas instalaciones eléctricas y de comunicación de los equipos.
- Inexistencia de un plan de contingencias en el caso de desastres naturales.

**CONTROLES FACTIBLES:**

- Realización de un mapa de ubicación y distribución de los equipos y del centro de cómputo, o del departamento de Informática.
- Se deberá monitorear constantemente el uso de los equipos.
- Adecuar las instalaciones eléctricas y de comunicación de los equipos.
- Elaboración de un plan de contingencias en prevención de desastres naturales.
- Hacer revisiones periódicas de las condiciones del local en prevención del desgaste de los equipos.

**RIESGO:**

c) Pérdida de los equipos.

**PROBLEMAS FACTIBLES:**

- Inexistencia de políticas de control de la seguridad física y vigilancia de los equipos.
- Ser susceptibles a sabotaje y robo de los equipos.
- Falta de inventarios confiables del equipo de cómputo.
- Falta de una persona responsable del equipo.

**CONTROLES FACTIBLES:**

- Definición de políticas para el control de la seguridad física de los equipos.
- Vigilancia continua en el centro de cómputo.
- Revisiones y actualizaciones periódicas de los inventarios de los equipos.
- Responsabilizar a una o varias personas por los equipos.

## EVALUACIÓN DE LA INFORMACIÓN.

### 1.- Control de entrada/ procesos/ salidas

**RIESGO:**

a) Resultados incongruentes.

**PROBLEMAS FACTIBLES:**

- Falta de revisión de la autenticidad de la información recibida para su captura.
- Captura de datos incorrectos.
- Inexistencia de procedimientos documentados <manuales> que expliquen la manera en que se introducen los datos.
- Falta de capacitación al personal.

**CONTROLES FACTIBLES:**

- Revisión de la autenticidad de la información antes de ser capturada.
- Existencia de un proceso de validación de datos de entrada.
- Existencia de la documentación de los procedimientos de manejo de errores.
- Existencia de manuales, que expliquen la manera en que se introducen los datos.
- Capacitar al personal encargado de capturar la información.

**RIESGO:**

b). Alteración en la integridad del procesamiento de datos.

**PROBLEMAS FACTIBLES:**

- Inexistencia de procedimientos documentados <manuales> que expliquen la manera en que se procesan los datos.
- Inexistencia de controles de procesamiento para evitar errores como:

  No investigación de cualquier desviación del operador con respecto a los procedimientos establecidos.

  No uso de contadores de lotes de datos procesados.

  No uso de contadores de registro de datos procesados.

  No uso de totales de control de datos procesados.
- Inexistencia de controles de procesamiento para evitar caídas del sistema.
- Lentitud en el procesamiento de los datos.

**CONTROLES FACTIBLES:**

- Determinar si existen procedimientos documentados que expliquen la manera en que se procesan los datos.
- Determinar si existen controles de procesamiento para evitar errores.
- Verificar si existen controles de procesamiento para evitar caídas del sistema.
- Realizar un análisis para satisfacer los requerimientos de velocidad.

**RIESGO:**

c). Complejidad para interpretar los resultados.

**PROBLEMAS FACTIBLES:**

- Mal diseño de reportes
- Despliegue de información innecesaria
- Formato de salida poco amigable

**CONTROLES FACTIBLES:**

- Definir estándares para el diseño de salidas
- Identificar los datos específicos de salida
- Seleccionar los métodos para la presentación de la información

**2.- Acceso a la información**

**RIESGO:**

a). Pérdida de Información

**PROBLEMAS FACTIBLES:**

- Acceso al personal no autorizado
- Falta de capacitación del personal
- Inadecuada organización de trabajo
- Fallas en el sistema de respaldo
- Errores del usuario
- No actualizaciones de respaldo

**CONTROLES FACTIBLES:**

- Implementar políticas de acceso a lugares donde se encuentra la información
- Monitorear el cumplimiento de las políticas de acceso a lugares donde se encuentra la información.
- Implementar el uso de vigilancia en lugares clave
- Capacitación al personal que está relacionado con el manejo de la Información.
- Establecer turnos de trabajo
- Hacer revisiones continuas a los sistemas de respaldo
- Establecer una excelente capacitación al personal de sistemas de respaldo
- Establecer una bitácora de actualizaciones de respaldos

**3.- Cuidado de la información.**

**RIESGO:**

a). Pérdida de la información.

**PROBLEMAS FACTIBLES:**

- Inexistencia de un plan de contingencias en caso de catástrofe.
- Inexistencia de equipo para evitar interrupciones de energía.
- Falta de Calendarización para la generación de respaldos, archivos y programas
- Inexistencia de respaldos fuera del departamento de Informática (Copias internas).
- Inexistencia de respaldos actualizados fuera de las instalaciones.
- Falta de etiquetas externas de identificación a los discos, cintas y diskettes.
- Falta de realización de pruebas con el material de respaldo.
- Material de respaldo inaccesible a cualquier hora.

- Falta de capacitación y supervisión a los usuarios.
- Inexistencia o no uso de un sistema de claves de acceso.
- Falta de detección de accesos no autorizados.
- Inexistencia de políticas para la ubicación del equipo.
- Falta de capacitación al personal encargado de respaldar.

**CONTROLES FACTIBLES:**

- Existencia de un plan de contingencias (que acciones ejecutar cuando exista alguna catástrofe).
- Existencia de equipo no "breack" (sistema de energía ininterrumpida).
- Establecer políticas de respaldo de información.
- Calendarización para la generación de respaldos, archivos y programas.
- Hacer revisiones continuas a los sistemas de respaldo.
- Existencia de respaldos fuera del departamento de Informática (Copias internas de protección, almacenadas en un sólo lugar).
- Existencia de respaldos actualizados fuera de las instalaciones.
- Etiquetas externas de identificación a los discos, cintas y diskettes.
- Realización de pruebas con el material de respaldo.
- Accesibilidad de material de respaldo a cualquier hora.
- Capacitar a todos los usuarios para tener la seguridad correcta de su trabajo.
- Auxiliar y supervisar a todos los usuarios, para tener la seguridad del desarrollo correcto de su trabajo.
- Proteger la información con claves de acceso e identificación de cada usuario.
- Detección de accesos no autorizados.
- Establecer políticas de ubicación del equipo.
- Capacitar al personal encargado de respaldar la información.

**4.- Calidad de la información**

**RIESGO:**

a). Dificultad en la interpretación de los datos para la toma de decisiones.

**PROBLEMAS FACTIBLES:**

- Nula consistencia en la presentación de la información.

**CONTROLES:**

- Establecer procedimientos en la presentación de la información.

**RIESGO:**

b). Insatisfacción del usuario.

**PROBLEMAS FACTIBLES:**

- Información deficiente.

**CONTROLES FACTIBLES:**

- Establecer medidas formales mediante una función de control de calidad de la información.
- Monitorear el grado de satisfacción del usuario en lo que se refiere a los servicios proporcionados por la función de sistemas de información.

*CUARTA ETAPA.*

*FASE: REPORTE FINAL.*

*DESARROLLO DE TAREAS.*

*1.- Interpretar la información obtenida para cada área analizada.*

Se realiza el análisis de la información obtenida la cual consiste en seguir los siguientes pasos :

- Argumentos del análisis.
- Riesgos factibles y su evaluación.
- Controles recomendados.
- Definir políticas de seguimiento de uso de controles.

## ARGUMENTOS DEL ANÁLISIS

*(DEPARTAMENTO DE INFORMATICA)*

A continuación se presenta un ejemplo representativo del caso práctico:

**1. ORGANIZACIÓN DEL ÁREA.**

RIESGO: A) INCUMPLIMIENTO DE LOS OBJETIVOS DE LA ORGANIZACIÓN DEL DEPARTAMENTO DE INFORMÁTICA.

- **Dar a conocer adecuadamente los objetivos de la Organización al personal del departamento de Informática.**

1. El personal de Informática no conoce los objetivos de las Organización.
2. Encontramos que no todo el personal de Informática conoce los objetivos del departamento.

**2. PRESUPUESTOS/GASTOS.**

RIESGO: A) PRESUPUESTOS INSUFICIENTES.

- **El Director de Informática vigilará que se realice una buena planeación de los presupuestos y gastos.**

1. Los Presupuestos/Gastos son planeados por el Director de Informática conforme los procedimientos establecidos en la institución ya que se trata de una Institución Gubernamental.

**3. PERSONAL EXTERNO.**

RIESGO: A) RESISTENCIA A LOS CAMBIOS Y USO DE TECNOLOGÍA.

- **Definir las funciones del departamento de Informática y darlas a conocer al personal externo.**

1. El personal externo no conoce las funciones del departamento de Informática.
2. El personal externo menciona como única función del departamento de Informática el soporte que les da a ellos.

3. El personal externo menciona que no considera necesario conocer las funciones del departamento de Informática.

**4. PERSONAL DE INFORMÁTICA.**

RIESGO: A) MAL AMBIENTE DE TRABAJO.

- **Tomar medidas para crear un buen ambiente de trabajo(buena integración y convivencia entre individuos.**

1. El Director de Informática toma como medidas para el buen ambiente de trabajo el buen trato y lo cordialidad.
2. El personal de Informática está integrado como grupo de trabajo.
3. La relación y convivencia en el departamento de Informática es informal.

**ARGUMENTOS DE ANÁLISIS**

**SOFTWARE**

**1. CONTROL DE PROYECTOS.**

RIESGO: A) PÉRDIDA DE INFORMACIÓN Y DE TIEMPO A CAUSA DE ERRORES EN LOS SISTEMAS.

- **Elaborar pruebas exhaustivas de todos los programas que intervienen en un nuevo sistema o que han sido modificados.**

1.- El departamento de Informática elabora las pruebas necesarias a los programas, para que estos no tengan ningún problema posterior a su instalación.

2.- El personal de Informática conoce los lenguajes de programación que utilizan para ella.

3.- El personal de Informática se encuentra relacionado con todos los sistemas instalados, por ende sabe dar el mantenimiento adecuado.

## 2.- ETAPAS DEL DESARROLLO DEL SISTEMA

RIESGO: A) ELABORAR UN PROYECTO DEFICIENTE.

- **Establecer adecuados canales formales de comunicación entre los empleados de la Organización.**

1.- No existe en la Organización, comunicación formal entre los empleados de la Organización y el departamento de Informática.

2.- Se tiene comunicación informal, por lo tanto la información de las necesidades de los departamentos es verbal.

## 3. MONITOREO DE SISTEMAS

RIESGO: A) SOFTWARE OBSOLETO.

- **Revisión periódica del crecimiento y desarrollo de la Organización para la adecuación de las necesidades del software a las mismas.**

1.- No se cuenta con el personal y tiempo para realizar periódicamente una supervisión del crecimiento y desarrollo de la Organización.

2.- Los jefes de departamentos solicitan el software que crean necesario para ayuda en su trabajo.

## 4. ADQUISICIÓN DEL SOFTWARE.

RIESGO: A) INCOMPATIBILIDAD DEL SOFTWARE ADQUIRIDO CON EL HARDWARE EXISTENTE.

- **Realizar una adecuada detección de necesidades y compatibilidad del software con el hardware.**

1.- No se cuenta con el personal y tiempo necesario para realizar una detección de necesidades a fondo.

2.- El departamento de Informática cuenta con los conocimientos necesarios sobre el hardware que tiene la Organización, por lo que siempre sabe que software les puede servir.

## ARGUMENTOS DEL ANÁLISIS EN LA EVALUACIÓN DE LOS EQUIPOS (HARDWARE)

1.- ADQUISICIÓN.

RIESGO : A) ELECCIÓN ERRÓNEA DE LOS EQUIPOS.

- **Definir políticas de adquisición y rendimiento de los equipos.**

1. No existen políticas de adquisición y rendimiento de los equipos correctamente documentadas pero si se llevan acabo durante el proceso de adquisición de los equipos.

**2. MANTENIMIENTO.**

RIESGO: A) BAJO O NULO RENDIMIENTO DE LOS EQUIPOS.

- **Contar con personal capacitado para el mantenimiento de los equipos.**

1. La persona encargada del mantenimiento de los equipos sí está capacitada.

**3. CONTROL DE FALLAS.**

RIESGO: A) ACUMULACIÓN Y SOBRECARGAS DE TRABAJO.

- **Elaboración de un plan efectivo de control de fallas.**

1. No existe un plan de control de fallas de las equipos.
2. Las fallas se solucionan conforme se van presentando.

**4. USO DE LOS EQUIPOS.**

RIESGO: A) MALTRATO O TRATO INADECUADO DE LOS EQUIPOS.

- **Capacitar a los usuarios en el uso y funcionamiento**

1. Los usuarios de los equipos reciben muy poca capacitación en el uso y funcionamiento de los equipos.
2. Algunos usuarios no reciben capacitación.
3. Algunos usuarios reciben capacitación por iniciativa propia.

## ARGUMENTOS DEL ANÁLISIS DEL ÁREA DE INFORMACIÓN

**1. CONTROL DE ENTRADA/ PROCESOS/ SALIDAS.**

RIESGO: A) RESULTADOS INCONGRUENTES.

- **Revisión de la autenticidad de la información antes de ser capturada.**

1.- La revisión de la información se lleva a cabo de manera minuciosa analizando su veracidad.

**2. ACCESO A LA INFORMACIÓN.**

RIESGO: A) PÉRDIDA DE INFORMACIÓN.

- **Implementar políticas de acceso a lugares donde se encuentra la información.**

1.- Existen algunas políticas de acceso, pero no están documentadas.

2.- Se cuenta con políticas de acceso permanente en el ámbito general, es decir, para todos los departamentos.

### 3. CUIDADO DE LA INFORMACIÓN.

RIESGO: A) PÉRDIDA DE LA INFORMACIÓN.

- **Existencia de un plan de contingencias (que acciones ejecutar cuando exista alguna catástrofe).**

1.- Sí existe un plan de contingencias.

2.- Se cuenta con poco tiempo de implantación.

### 4. CALIDAD DE LA INFORMACIÓN

RIESGO: A) DIFICULTAD EN LA INTERPRETACIÓN DE LOS DATOS PARA LA TOMA DE DECISIONES.

- **Establecer procedimientos en la presentación de la información.**

1.- Se lleva a cabo procedimientos en la presentación de la información.

## RIESGOS FACTIBLES Y SU EVALUACIÓN (Departamento de Informática)

### *1.- Evaluación de Organización del Área.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Incumplimiento de objetivos de la Organización por parte del Departamento de Informática. | Dar a conocer adecuadamente los objetivos de la Organización al personal del departamento de Informática. | | ✓ | | | |
| | Objetivos del departamento congruentes con los de la Organización. | | | | ✓ | |
| | Monitoreo del cumplimiento de los objetivos por parte del personal del departamento. | | ✓ | | | |
| b) Incumplimiento de los objetivos del departamento de Informática. | El Director de Informática definirá los objetivos del departamento de Informática basándose en los de la Organización en general. | | | | ✓ | |
| | El Director de Informática difundirá y validara constantemente los objetivos del departamento. | | ✓ | | | |
| c) Mal funcionamiento del departamento de Informática | Definir políticas y monitorear su funcionamiento | | ✓ | | | |
| | Definir políticas de selección de personal. | | | ✓ | | |
| | Brindar capacitación adecuada y constante. | | ✓ | | | |
| | Llevar un correcto control anual de gastos para definir presupuestos confiables. | | | | | ✓ |
| d) Crear una mala imagen del departamento de Informática ante los demás miembros de la Organización. | Crear un plan prioritario de las actividades de los departamentos dependientes del departamento de Informática. | | | | | ✓ |
| | Proporcionar un soporte eficaz a los departamentos que lo requieran. | | | | ✓ | |
| | Contar con personal bien capacitado. | | | | ✓ | |
| e) Mala definición de proyectos. | Hacer la ubicación correcta de departamento de Informática. | | ✓ | | | |
| | El Director de Informática conocerá los objetivos de la Organización. | | | | ✓ | |
| | El Director de Informática conocerá perfectamente el alcance del departamento. | | | | | ✓ |
| | El departamento de Informática contará con un plan bien definido de cargas de trabajo y asignación de tiempos de proyectos. | | | ✓ | | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.2** Riesgos factibles y su evaluación (Organización del área).

## *2. Presupuestos y gastos.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Presupuestos insuficientes. | El Director de Informática vigilara que se realice una buena planeación de los presupuestos y gastos. | | | | | ✓ |
| | Elaboración de presupuestos flexibles. | ✓ | | | | |
| | Crear un fondo de contingencias. | ✓ | | | | |
| | Realizar revisiones periódicas del plan de contingencias en caso de que ya exista. | ✓ | | | | |
| B) Surgimiento de gastos imprevistos. | Se proporcionará capacitación para la elaboración de presupuestos. | ✓ | | | | |
| | Manejo adecuado del recurso humano. | ✓ | | | | |
| | El Director de Informática llevará un buen manejo y Administración de las presupuestos y de los gastos. | | | | | ✓ |
| C) Presupuestos /Gastos no aprobados. | Elaborar buenos y eficaces presupuestos. | | | | | ✓ |
| | Elaborar presupuestos con técnicas probadas y confiables. | | | | | ✓ |
| | Establecer una supervisión continua en la elaboración de los presupuestos. | | | | ✓ | |
| D) Sobrestimación del presupuesto. | Aplicación de técnicas confiables en la planeación del presupuesto. | | | | ✓ | |
| | Apegarse a las partidas presupuestales | | | | | ✓ |
| | Supervisar estrictamente la utilización de las partidas. | | | | | ✓ |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.3** Riesgos factibles y su evaluación (Presupuestos y gastos).

### *3. Personal Externo.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Resistencia a los cambios y uso de tecnología avanzada. | Definir las funciones del departamento de Informática y darlas a conocer al personal externo. | | ✓ | | | |
| | Inducir al personal de Informática por medio de cursos para lograr buena comunicación con el personal externo. | | ✓ | | | |
| | Levar a cabo programas de capacitación para proporcionar el soporte técnico que demanda el personal externo. | | ✓ | | | |
| | Desarrollar actividades involucrando al personal externo | ✓ | | | | |
| B) Mal uso de los recursos de Informática. | Capacitar al personal externo sobre el uso y cuidado de los equipos. | | ✓ | | | |
| | Monitorear al personal externo ante su trabajo. | | | ✓ | | |
| | Evaluar al personal de Informática en cuanto al soporte que le proporciona al personal externo. | | | | ✓ | |
| C) Personal Externo ineficiente en su trabajo. | Proporcionar capacitación adecuada al per sonal Externo. | | ✓ | | | |
| | Difundir las políticas y funciones para el uso correcto de los equipos. | | ✓ | | | |
| | Implantación de sistemas con ambiente amigable para el usuario. | | | | | ✓ |
| | Supervisión continua al personal externo. | | | ✓ | | |
| | Mantener óptimas las condiciones ambientales de la Organización. | | | ✓ | | |
| | Realizar dinámicas de grupos para mejorar las relaciones entre personas. | | | ✓ | | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.4** Riesgos factibles y su evaluación (Personal externo).

### *4. Personal de Informática.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Mal ambiente de trabajo | Tomar medidas para crear un buen ambiente de trabajo(buena integración y convivencia entre individuos). | | | | ✓ | |
| | Contar con buenas condiciones ambientales en las instalaciones del edificio de la Organización. | | | ✓ | | |
| b) Mal desempeño y comportamiento del personal. | Utilizar técnicas eficientes, para la elección del personal. | | | | | ✓ |
| | Imponer reglas eficaces para una buena disciplina. | | | | ✓ | |
| | Realizar un buen control de tareas. | | | ✓ | | |
| | Asignar responsabilidades y delimitar la autoridad. | | | ✓ | | |
| C) Malas condiciones de trabajo | Distribuir el reglamento interno de trabajo. | | | ✓ | | |
| | Lograr que el personal se sienta satisfecho y bien remunerado económicamente. | | ✓ | | | |
| d) Mala organización en el trabajo. | Elaboración de programas para anticipar las necesidades del área. | | | ✓ | | |
| | Realizan un buen reclutamiento y selección del personal. | | | | ✓ | |
| e) Mal desarrollo y motivación del personal. | Definir programas de motivación, recompensas, y ascensos para el personal. | | ✓ | | | |
| F) Mala capacitación del personal. | Identificar las necesidades actuales y futuras de capacitación de personal. | | | ✓ | | |
| | Elaboración de programas de capacitación. | | | ✓ | | |
| | Proporcionar la capacitación al personal. | | ✓ | | | |
| | Verificación de los resultados de las capacitaciones. | | ✓ | | | |

N = nunca D= deficiente A = aceptable G = generalmente S = siempre.

**Tabla VI.5** Riesgos factibles y su evaluación (Personal de Informática).

## RIESGOS FACTIBLES Y SU EVALUACIÓN ( Software).

### *1.- Control de proyectos.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Pérdida de información y de tiempo a causa de errores en los sistemas | Elaborar pruebas exhaustivas de todos los programas que intervienen en un nuevo sistema o que han sido modificados. | | | | ✓ | |
| | Realizar análisis y diseño de los sistemas. | | | ✓ | | |
| b) Retraso en la presentación de reportes | Tener un diseño en el sistema lo más óptimo posible y estructurado. | | | | | ✓ |
| | Contar con un acceso inmediato a los procesos que generen los reportes. | | | ✓ | | |
| c) Excesivo costo en el desarrollo del sistema | Elección adecuada del personal para la elaboración del presupuesto. | | | | ✓ | |
| | Capacitación eficiente del personal. | | | | ✓ | |
| | Evaluación y elaboración del costo/beneficio | | | | ✓ | |
| d) Dificultad para realizar el mantenimiento del sistema | Establecer políticas de documentación de los sistemas | | ✓ | | | |
| | Seleccionar personal capacitado | | | | | ✓ |
| e) El programa no cumpla con los objetivos del proyecto. | Definir la finalidad del sistema correctamente en la etapa del análisis | | | ✓ | | |
| | Elección de un buen equipo de trabajo preparado profesionalmente | | | | | ✓ |
| | Establecimiento previo de estándares a manejar en todo el ciclo de vida del sistema | | | | ✓ | |
| | El directivo eligirá al personal clave para proporcionar información verídica y completa | | | ✓ | | |
| | Tomar en cuenta todas las áreas que estarán con el sistema | | | | ✓ | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.6** Riesgos factibles y su evaluación (Control de proyectos).

## *2.- Etapas de desarrollo del sistema*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Elaborar un proyecto deficiente. | Establecer adecuados canales formales de comunicación entre los empleados de la Organización. | | ✓ | | | |
| | Elaborar una adecuada planeación y cumplir con los tiempos señalados. | | | ✓ | | |
| | Previamente el operario deberá conocer el funcionamiento y actividades que en forma Genérica realiza la Organización. | | | | ✓ | |
| | Contar con una adecuada distribución del trabajo, para tener una buena organización y con esto dar como resultado una armonía en le trabajo. | | | | ✓ | |
| b) Error en el manejo de los archivos | Definir un programa de trabajo para determinar el tipo y la frecuencia de protección de los datos de acuerdo a su naturaleza y utilización. | | | | | ✓ |
| c) Incumplimiento en tiempos de entrega de los sistemas. | Elaboración e implantación de un cronograma de actividades. | ✓ | | | | |
| | Elección de un equipo de trabajo capacitado | | | | | ✓ |
| | Concluir todos los sistemas requeridos por la Organización | | | | | ✓ |
| | Elaborar una programación bien estructurada y hacerle pruebas de verificación | | | | | ✓ |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.7** Riesgos factibles y su evaluación (Etapas de desarrollo de sistemas).

### *3.- Monitoreo de sistemas*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Software obsoleto. | Revisión periódica del crecimiento y desarrollo de la Organización de las necesidades del software. | | | ✓ | | |
| b) Rechazo del usuario hacia el manejo de los sistemas. | Tener la autoridad de los altos funcionarios de la Organización para poder dar conjuntamente con el departamento de Recursos Humanos los cursos de capacitación pertinentes para los cambios de actitudes y aptitudes de los usuarios ante las innovaciones. | | | ✓ | | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.8** Riesgos factibles y su evaluación (Monitoreo de Sistemas).

### *4.- Adquisición del software*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Incompatibilidad del software adquirido con el hardware existente. | Realizar una adecuada detección de necesidades y compatibilidad del software con el hardware. | | | ✓ | | |
| | Elaborar y actualizar inventario del hardware que tenga la Organización y en el departamento de Informática. | | ✓ | | | |
| b) Incompatibilidad del software adquirido con el software existente. | Elaborar una adecuada detección de necesidades de software en los diversos departamentos de la Organización. | | | ✓ | | |
| | Elaborar y actualizar inventario del software que tenga la Organización y el departamento de Informática. | ✓ | | | | |
| c) Agotamiento del presupuesto antes de lo estimado. | Realizar un estudio de tiempo y movimientos evaluando al personal en cuanto al manejo de los recursos disponibles. | ✓ | | | | |
| | Capacitar al personal de la importancia que tiene el no dispendio de los recursos. | ✓ | | | | |
| | Realizar un estudio con los índices inflacionarios para prever la devaluación de costos de la adquisición de software a futuro. | ✓ | | | | |
| | Elaborar una adecuada planeación para la buena distribución del presupuesto. | | | ✓ | | |
| d) Invertir en software innecesario. | Contar con el inventario actualizado del software y con esto saber que es lo necesario y adecuado para la excelente utilización en la empresa y que exista una mayor eficacia y eficiencia. | ✓ | | | | |
| | Asignación de un responsable para que determine que software se va adquirir o se requiere dependiendo lo que exista en el mercado. | | | ✓ | | |
| e) Invertir en software necesario y no utilizarlo. | Capacitar al usuario sobre el nuevo software adquirido. | | ✓ | | | |
| | Asignación del capacitador y del personal que recibirá capacitación | | | ✓ | | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.9** Riesgos factibles y su evaluación (Adquisición del software).

## RIESGOS FACTIBLES Y SU EVALUACIÓN (Hardware).

### *1. Adquisición.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Elección errónea de los equipos. (Funcionalidad - Rendimiento). | Definir políticas de adquisición y rendimiento de los equipos. | | | ✓ | | |
| | Realizar programas de adquisición y rendimiento de los equipos. | | | ✓ | | |
| | Revisiones y actualizaciones periódicas de los inventarios de los equipos. | | ✓ | | | |
| B) Utilización de procedimientos erróneos. | Realizar concursos para elegir al proveedor correcto de los equipos de cómputo | | | | ✓ | |
| | El Director de Informática supervisará el proceso de compra de los equipos. | | | | | ✓ |
| c) Mal pronostico del costo-beneficio. | Supervisar al personal que realizará los estudios costo-beneficio del departamento. | | ✓ | | | |
| | Verificar que el personal esté realmente capacitado en el área. | | | ✓ | | |
| | Realizar estudios profundos de factibilidad económica, operativa y tecnológica para la adquisición de los equipos de cómputo. | | | ✓ | | |

N = nunca D= deficiente A = aceptable G = generalmente S = siempre.

**Tabla VI.10** Riesgos factibles y su evaluación (Adquisición de equipo).

### *2. Mantenimiento.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Bajo o nulo rendimiento de los equipos. | Contar con personal capacitado para el mantenimiento de los equipos. | | | | ✓ | |
| | Contar con el número adecuado de personal para el mantenimiento de los equipos. | | ✓ | | | |
| | Contar con un buen programa de mantenimiento. | | | | ✓ | |
| | Monitorear el cumplimiento del mantenimiento de los equipos. | | | ✓ | | |
| b) Mal mantenimiento. | Definición de las políticas de mantenimiento de los equipos. | | | ✓ | | |
| | Realización de registros del mantenimiento de los equipos. | | | | ✓ | |
| | Realización de presupuestos correctos para la inversión que requiere el mantenimiento de los equipos. | | | | | ✓ |

N = nunca D= deficiente A = aceptable G = generalmente S = siempre. ** = No procede.

**Tabla VI.11** Riesgos factibles y su evaluación (Mantenimiento).

### *3. Control de fallas.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Acumulación y sobrecargas de trabajo. | Elaboración de un plan efectivo de control de fallas. | ✓ | | | | |
| | Poner en práctica y monitorear periódicamente el plan preventivo de fallas. | ✓ | | | | |
| | Elaboración de reportes sobre las fallas. | | | ✓ | | |
| | Contar con personal capacitado para reparar las fallas. | | | | ✓ | |
| | Contar presupuesto para refacciones y reparar las fallas. | ✓ | | | | |
| | Concientizar a los usuarios de los equipos de la importancia de tratar adecuadamente el equipo de cómputo. | | | | ✓ | |
| b) Pérdida de tiempo de los usuarios. | Realización de cronogramas de control de fallas. | ✓ | | | | |
| | Bitácora de ajuste de los equipos. | ✓ | | | | |
| c) Pérdida de dinero para la Organización. | Supervisión continua del control de fallas. | | ✓ | | | |
| | Realización de un buen presupuestos para el gasto que ocasiona la reparación de fallas. | | ✓ | | | |
| d) Caídas de la red del centro de cómputo. | Contar con la protección de baterías (UPS) para evitar la caída de la red. | | | ✓ | | |
| | Contar con instalaciones físicas de la red apropiadas.( Cable protegido de pisarlo, de mordeduras de ratas etc.). | | ✓ | | | |
| | Definir correctamente las políticas para el control de fallas de la red. | | | ✓ | | |

N = nunca D= deficiente A = aceptable G = generalmente S = siempre.

**Tabla VI.12** Riesgos factibles y su evaluación (Control de fallas).

### *4. Uso de los equipos.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Maltrato o trato inadecuado de los equipos. | Capacitar a los usuarios en el uso y funcionamiento. | | ✓ | | | |
| | Restringir el acceso a los equipos de personal ajeno a ellos. | | | | ✓ | |
| | Contar con vigilancia permanente de los equipos. | | | ✓ | | |
| b) Maltrato o desgaste por el ambiente natural. | Realización de un mapa de ubicación y distribución de los equipos y del centro de cómputo o departamento de Informática. | | | ✓ | | |
| | Se deberá monitorear constantemente el uso de los equipos. | | | ✓ | | |
| | Adecuar las instalaciones eléctricas y de comunicación de los equipos. | | | ✓ | | |
| | Elaboración de un plan de contingencias en prevención de desastres naturales. | | | | | ✓ |
| | Hacer revisiones periódicas de las condiciones del local en prevención del desgaste de los equipos. | | | ✓ | | |
| c) Pérdida de los equipos. | Definición de políticas para el control de la seguridad física de los equipos . | | | ✓ | | |
| | Responsabilizar a una o varias personas por los equipos y su uso. | | | | ✓ | |
| | Vigilancia continua en el centro de cómputo . | | | ✓ | | |

N = nunca D= deficiente A = aceptable G = generalmente S = siempre.

**Tabla VI.13** Riesgos factibles y su evaluación (Uso de los equipos).

## RIESGOS FACTIBLES Y SU EVALUACIÓN (Información).

### *1.- Control de entradas/procesos/salidas.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Resultados incongruentes. | Revisión de la autenticidad de la información antes de ser capturada. | | | | | ✓ |
| | Existencia de un proceso de validación de datos de entrada. | | | | | ✓ |
| | Existencia de la documentación de los procedimientos de manejo de errores. (entrada) | | | | | ✓ |
| | Existencia de manuales, que expliquen la manera en que se introducen los datos. | | ✓ | | | |
| | Capacitar al personal encargado de capturar la información. | | ✓ | | | |
| b) Alteración en la integridad del procesamiento de datos . | Determinar si existen procedimientos documentados que expliquen la manera en que se procesan los datos. | | ✓ | | | |
| | Determinar si existen controles de procesamiento para evitar errores. | | | ✓ | | |
| | Realizar un análisis para satisfacer los requerimientos de velocidad. | | | ✓ | | |
| c) Complejidad para interpretar los resultados. | Definir estándares para el diseño de salidas. | | | | | ✓ |
| | Identificar los datos específicos de salida. | | | | | ✓ |
| | Seleccionar los métodos para la presentación de la información. | | | | | ✓ |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.14** Riesgos factibles y su evaluación (Control de entradas/ procesos y salidas).

## *2.- Acceso a la información.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Pérdida de información. | Implementar políticas de acceso a lugares donde se encuentra la información. | | | ✓ | | |
| | Monitorear el cumplimiento de las políticas de acceso a lugares donde se encuentra la información. | | | ✓ | | |
| | Implementar el uso de vigilancia en lugares claves. | | | ✓ | | |
| | Capacitación al personal que está relacionado con el manejo de la información. | | ✓ | | | |
| | Establecer turnos de trabajo. | | | | | ✓ |
| | Hacer revisiones continuas a los sistemas de respaldo. | ✓ | | | | |
| | Establecer una excelente capacitación al personal de sistemas de respaldo. | | | ✓ | | |
| | Establecer una bitácora de actualizaciones de respaldo. | | | | | ✓ |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.15** Riesgos factibles y su evaluación (Acceso a la Información).

### *3.- Cuidado de la Información.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Pérdida de la información. | Existencia de un plan de contingencias. | | | ✓ | | |
| | Existencia de equipo no "breack". | | | ✓ | | |
| | Establecer políticas de respaldo de información. | | | ✓ | | |
| | Calendarización para la generación de respaldos, archivos y programas. | | | | | ✓ |
| | Hacer revisiones continuas a los sistemas de respaldo. | ✓ | | | | |
| | Existencia de respaldos fuera del departamento de Informática | | | | | ✓ |
| | Existencia de respaldos actualizados fuera de las instalaciones. | | | ✓ | | |
| | Etiquetas externas de identificación a los discos, cintas y diskettes. | | | | | ✓ |
| | Realización de pruebas con el material de respaldo. | ✓ | | | | |
| | Accesibilidad de material de respaldo a cualquier hora. | | | | ✓ | |
| | Capacitar a todos los usuarios para el desarrollo correcto de su trabajo. | | ✓ | | | |
| | Auxiliar y supervisar a todos los usuarios, para tener la seguridad del desarrollo correcto de su trabajo. | | | | | ✓ |
| | Proteger la información con claves de acceso e identificación de cada usuario. | | | | | ✓ |
| | Detección de accesos no autorizados. | | | | | ✓ |
| | Capacitar al personal encargado de respaldar la información. | | | ✓ | | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.16** Riesgos factibles y su evaluación (Cuidado de la Información).

### *4.- Calidad de la Información.*

| *RIESGOS* | *CONTROLES* | *N* | *D* | *A* | *G* | *S* |
|---|---|---|---|---|---|---|
| a) Dificultad en la interpretación de los datos para la toma de decisiones. | Establecer procedimientos en la presentación de la información. | | | | ✓ | |
| b) Insatisfacción del usuario. | Monitorear el grado de satisfacción del usuario en lo que se refiere a los servicios proporcionados por la función de sistemas de información. | ✓ | | | | |

N = Nunca D= Deficiente A = Aceptable G = Generalmente S = Siempre.

**Tabla VI.17** Riesgos factibles y su evaluación (Calidad de la Información).

## *CONTROLES RECOMENDADOS.*

**Controles recomendados**

***Área de:*** Departamento de Informática.

***Sub área:*** Organización del área

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Incumplimiento de objetivos de la Organización por parte del departamento de Informática. | Dar a conocer adecuadamente los objetivos de la Organización al personal del departamento de Informática. | | ☑ |
| | Objetivos del departamento congruentes con los de la Organización. | ☑ | |
| | Monitoreo del cumplimiento de los objetivos por parte del personal del departamento. | | ☑ |
| b) Incumplimiento de los objetivos del departamento de Informática. | El Director de Informática definirá los objetivos del departamento de Informática en base a los de la Organización en general. | ☑ | |
| | El Director de Informática difundirá y validará constantemente los objetivos del departamento. | | ☑ |
| c) Mal funcionamiento del departamento de Informática | Definir políticas y monitorear su funcionamiento | | ☑ |
| | Definir políticas de selección de personal. | ☑ | |
| | Brindar capacitación adecuada y constante. | | ☑ |
| | Llevar un correcto control anual de gastos para definir presupuestos confiables. | ☑ | |
| d) Crear una mala imagen del departamento de Informática ante los demás miembros de la Organización. | Crear un plan prioritario de las actividades de los departamentos dependientes del departamento de Informática. | | ☑ |
| | Proporcionar un soporte eficaz a los departamentos que lo requieran. | ☑ | |
| | Contar con personal bien capacitado. | ☑ | |
| e) Mala definición de proyectos. | Hacer la ubicación correcta de departamento de Informática. | | ☑ |
| | El Director de Informática conocerá los objetivos de la Organización. | ☑ | |
| | El Director de Informática conocerá perfectamente el alcance del departamento. | ☑ | |
| | El departamento de Informática contará con un plan bien definido de cargas de trabajo y asignación de tiempos de proyectos. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.18** Controles recomendados (Organización del área).

## *Controles recomendados*

***Área de:*** Departamento de Informática.

***Sub área:*** Presupuestos/ Gastos.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Presupuestos insuficientes. | El Director de Informática vigilará que se realice una buena planeación de los presupuestos y gastos. | ☑ | |
| | Elaboración de presupuestos flexibles. | | ☑ |
| | Crear un fondo de contingencias. | | ☑ |
| | Realizar revisiones periódicas del plan de contingencias en caso de que ya exista. | | ☑ |
| B) Surgimiento de gastos imprevistos. | Se proporcionará capacitación para la elaboración de presupuestos. | | ☑ |
| | Manejo adecuado del recurso Humano. | | ☑ |
| | El Director de Informática llevará un buen manejo y Administración de las presupuestos y de los gastos. | ☑ | |
| C) Presupuestos /Gastos no aprobados. | Elaborar buenos y eficaces presupuestos. | ☑ | |
| | Elaborar presupuestos con técnicas probadas y confiables. | ☑ | |
| | Establecer una supervisión continua en la elaboración de los presupuestos. | ☑ | |
| D) Sobrestimación del presupuesto. | Aplicación de técnicas confiables en la planeación del presupuesto. | ☑ | |
| | Apegarse a las partidas presupuestales | ☑ | |
| | Supervisar estrictamente la utilización de las partidas. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.19** Controles recomendados (Presupuestos y gastos).

## *Controles recomendados*

***Área de:*** Departamento de Informática.

***Sub área:*** Personal externo.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Resistencia a los cambios y uso de tecnología avanzada. | Definir las funciones del departamento de Informática y darlas a conocer al personal externo. | | ☑ |
| | Inducir al personal de Informática por medio de cursos para lograr buena comunicación con el personal externo. | | ☑ |
| | Levar a cabo programas de capacitación para proporcionar el soporte técnico que demanda el personal externo. | | ☑ |
| | Desarrollar actividades involucrando al personal externo | | ☑ |
| B) Mal uso de los recursos de Informática. | Capacitar al personal externo sobre el uso y cuidado de los equipos. | | ☑ |
| | Monitorear al personal externo ante su trabajo. | | ☑ |
| | Evaluar al personal de Informática en cuanto al soporte que le proporciona al personal externo. | | ☑ |
| C) Personal Externo ineficiente en su trabajo. | Proporcionar capacitación adecuada al personal Externo. | | ☑ |
| | Difundir las políticas y funciones para el uso correcto de los equipos. | | ☑ |
| | Implantación de sistemas con ambiente amigable para el usuario. | ☑ | |
| | Supervisión continua al personal externo. | | ☑ |
| | Mantener óptimas las condiciones ambientales de la Organización. | | ☑ |
| | Realizar dinámicas de grupos para mejorar las relaciones entre personas. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.20** Controles recomendados (Personal externo).

## *Controles recomendados*

***Área de:*** Departamento de Informática.
***Sub área:*** Personal de Informática.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Mal ambiente de trabajo | Tomar medidas para crear un buen ambiente de trabajo(buena integración y convivencia entre individuos). | ☑ | |
| | Contar con buenas condiciones ambientales en las instalaciones del edificio de la Organización. | | ☑ |
| b) Mal desempeño y comportamiento del personal. | Utilizar técnicas eficientes, para la elección del personal. | ☑ | |
| | Imponer reglas eficaces para una buena disciplina. | ☑ | |
| | Realizar un buen control de tareas. | ☑ | |
| | Asignar responsabilidades y delimitar la autoridad. | | ☑ |
| C) Malas condiciones de trabajo | Distribuir el reglamento interno de trabajo. | | ☑ |
| | Lograr que el personal se sienta satisfecho y bien remunerado económicamente. | | |
| d) Mala organización en el trabajo. | Elaboración de programas para anticipar las necesidades del área. | ☑ | |
| e) Mal desarrollo y motivación del personal. | Definir programas de motivación, recompensas, y ascensos para el personal. | | ☑ |
| F) Mala capacitación del personal. | Identificar las necesidades actuales y futuras de capacitación de personal. | | ☑ |
| | Elaboración de programas de capacitación. | | ☑ |
| | Proporcionar la capacitación al personal. | | ☑ |
| | Verificación de los resultados de las capacitaciones. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.21** Controles recomendados (Personal de Informática).

**Controles recomendados**

***Área de:*** Software.
***Sub área:*** Control de Proyectos.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Pérdida de información y de tiempo a causa de errores en los sistemas. | Elaborar pruebas exhaustivas de todos los programas que intervienen en un sistema o que han sido modificados. | ☑ | |
| | Realiza un análisis más a fondo, para la elaboración de los sistemas. | | ☑ |
| b) retraso en la presentación de reportes | Tienen un diseño en el sistema lo más óptimo posible y estructurado. | ☑ | |
| | Contar con el acceso inmediato a los procesos que generan los reportes. | ☑ | |
| c) Excesivo costo en el desarrollo del sistema. | Elección adecuada del personal para evaluar el presupuesto. | ☑ | |
| | Capacitación eficiente del personal. | ☑ | |
| | Evaluación y elaboración del costo/beneficio. | ☑ | |
| d) Dificultad para realizar el mantenimiento del sistema. | Establecer políticas de documentación de los sistemas | | ☑ |
| e) El programa no cumpla con los objetivos del proyecto. | Definir la finalidad del sistema correctamente en la etapa del análisis | ☑ | |
| | Establecimiento previo de estándares a manejar en el ciclo de vida del sistema. | | ☑ |
| | El Directivo eligirá al personal clave para proporcionar información verídica y completa. | ☑ | |
| | Tomar en cuenta todas las áreas que estarán con el sistema. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.22** Controles recomendados (Control de Proyectos).

## ETAPAS DE DESARROLLO DEL SISTEMA

| *Controles recomendados*<br>***Área de:*** Software<br>***Sub área:*** Etapas de desarrollo | | | |
|---|---|---|---|
| ***RIESGOS*** | ***CONTROLES*** | ***E*** | ***R*** |
| a) Elaborar un proyecto deficiente. | Establecer adecuados canales formales de comunicación entre el usuario y el departamento de Informática. | | ☑ |
| | Elaborar una adecuada planeación y cumplir con los tiempos señalados. | | ☑ |
| | Previamente el programador deberá conocer el funcionamiento y actividades que en forma genérica realiza la Organización. | | ☑ |
| | Contar con una adecuada distribución del trabajo para tener armonía en el trabajo. | | ☑ |
| b) Error en el manejo de los archivos. | Definir un programa de trabajo para determinar el tipo y la frecuencia de protección de los datos de acuerdo a su naturaleza y utilización (archivos maestros, de transacciones, acumulados históricos, otros.). | | ☑ |
| | Concluir todos los sistemas requeridos por la Organización | | ☑ |
| | Elaborar una programación bien estructurada y hacer pruebas de verificación. | | ☑ |
| c) incumplimiento en tiempos de entrega de los sistemas. | Elaboración e implantación de un cronograma de actividades. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.23** Controles recomendados (Etapas de desarrollo del software).

| *Controles recomendados* | | | |
|---|---|---|---|
| ***Área de:*** Software. | | | |
| ***Sub área:*** Monitoreo de sistemas. | | | |
| ***RIESGOS*** | ***CONTROLES*** | ***E*** | ***R*** |
| a) Software obsoleto. | Revisión periódica del crecimiento y desarrollo de la Organización para la adecuación de las necesidades del software. | | ☑ |
| b) Rechazo del usuario hacia el manejo de los sistemas. | Tener la autorización de los altos funcionarios de la Organización para poder dar conjuntamente con recursos humanos los cursos de capacitación Pertinentes para los cambios de actitudes y aptitudes de los usuarios ante las innovaciones. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.24** Controles recomendados (Monitoreo de Sistemas).

**Controles recomendados**

***Área de:*** Software.
***Sub área:*** Adquisición de software.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Incompatibilidad del software adquirido con el hardware existente. | Realizar una adecuada detección de necesidades y compatibilidad del software con el hardware. | | ☑ |
| | Elaborar y actualizar un inventario del hardware, conque cuenta la Organización y en el departamento de Informática. | | ☑ |
| b) Incompatibilidad del software adquirido con el software existente. | Elaborar y actualizar inventario del software que tenga la Organización y el depto. de Informática. | | ☑ |
| c) Agotamiento de presupuesto antes de lo estimado | Realizar un estudio con los índices inflacionarios para prever la devaluación de costos de la adquisición del software a futuro. | | ☑ |
| | Elaborar una adecuada planeación para la buena distribución del presupuesto. | | ☑ |
| d) Invertir en software innecesario. | Contar con el inventario actualizado del software y con esto saber que es lo necesario y adecuado para la excelente utilización en la empresa y que exista una mayor eficiencia y eficacia. | | ☑ |
| e) Invertir en software necesario y no utilizarlo | Capacitar al usuario sobre el nuevo software adquirido. | | ☑ |
| | Asignación del capacitador y del personal que recibirá la capacitación. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.23** Controles recomendados (Adquisición del software).

**Controles recomendados**

***Área de:*** Equipos de cómputo (***Hardware***).

***Sub área:*** Adquisición.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Elección errónea de los equipos. (Funcionalidad - Rendimiento). | Definir políticas de adquisición y rendimiento de los equipos. | ☑ | |
| | Realizar programas de adquisición y rendimiento de los equipos. | ☑ | |
| | Revisiones y actualizaciones periódicas de los inventarios de los equipos. | | ☑ |
| b) Utilización de procedimientos erróneos. | El Director de Informática supervisará el proceso de compra de los equipos. | ☑ | |
| | Supervisar al personal que realizará los estudios costo-beneficio del departamento. | | ☑ |
| c) Mal pronóstico del costo-beneficio. | Verificar que el personal esté realmente capacitado en el área. | | ☑ |
| | Realizar estudios profundos de factibilidad económica, operativa y tecnológica para la adquisición de los equipos de cómputo. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.26** Controles recomendados (Adquisición de equipo).

***Controles recomendados***

***Área de:*** Equipos de Cómputo ( ***Hardware***).

***Sub área:*** Mantenimiento

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Bajo o nulo rendimiento de los equipos. | Contar con personal capacitado para el mantenimiento de los equipos. | ☑ | |
| | Contar con el número adecuado de personal para el mantenimiento de los equipos. | | ☑ |
| | Contar con un buen programa de mantenimiento. | ☑ | |
| | Monitorear el cumplimiento del mantenimiento de los equipos. | | ☑ |
| b) Mal mantenimiento. | Definición de las políticas de mantenimiento de los equipos. | ☑ | |
| | Realización de registros del mantenimiento de los equipos. | ☑ | |
| | Realización de presupuestos correctos para la inversión que requiere el mantenimiento de los equipos. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.27** Controles recomendados (Mantenimiento).

## *Controles recomendados*

***Área de:*** Equipos de Cómputo. (***Hardware***)
***Sub área:*** Control de Fallas.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Acumulación y sobrecargas de trabajo. | Elaboración de un plan efectivo de control de fallas. | | ☑ |
| | Poner en práctica y monitorear periódicamente el plan preventivo de fallas. | | ☑ |
| | Elaboración de reportes sobre las fallas. | | ☑ |
| | Contar con personal capacitado para reparar las fallas. | ☑ | |
| | Contar presupuesto para refacciones y reparar las fallas. | | ☑ |
| | Concientizar a los usuarios de los equipos de la importancia de tratar adecuadamente el equipo de cómputo. | ☑ | |
| b) Pérdida de tiempo de los usuarios. | Realización de cronogramas de control de fallas. | | ☑ |
| | Bitácora de ajuste de los equipos. | | ☑ |
| c) Pérdida de dinero para la Organización. | Supervisión continua del control de fallas. | | ☑ |
| | Realización de un buen presupuestos para el gasto que ocasiona la reparación de fallas. | | ☑ |
| d) Caídas de la red del centro de cómputo. | Contar con la protección de baterías (UPS) para evitar la caída de la red. | ☑ | |
| | Contar con instalaciones físicas de la red apropiadas.( Cable protegido de pisarlo, de mordeduras de ratas etc.). | | ☑ |
| | Definir correctamente las políticas para el control de fallas de la red. | | ☑ |

E = Controles existentes R = Controles recomendados

**Tabla VI.28** Controles recomendados (Control de fallas).

## *Controles recomendados*

***Área de:*** Equipos de cómputo. (***Hardware***).
***Sub área:*** Uso de los equipos.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Maltrato o trato inadecuado de los equipos. | Capacitar a los usuarios en el uso y funcionamiento de los equipos. | | ☑ |
| | Restringir el acceso a los equipos de personal ajeno a ellos. | ☑ | |
| | Contar con vigilancia permanente de los equipos. | ☑ | |
| b) Maltrato o desgaste por el ambiente natural. | Realización de un mapa de ubicación y distribución de los equipos y del centro de cómputo o departamento de Informática. | ☑ | |
| | Se deberá monitorear constantemente el uso de los equipos. | ☑ | |
| | Adecuar las instalaciones eléctricas y de comunicación de los equipos. | | ☑ |
| | Elaboración de un plan de contingencias en prevención de desastres naturales. | ☑ | |
| | Hacer revisiones periódicas de las condiciones del local en prevención del desgaste de los equipos. | ☑ | |
| c) Pérdida de los equipos. | Definición de políticas para el control de la seguridad física de los equipos . | ☑ | |
| | Responsabilizar a una o varias persona por los equipos y su uso. | ☑ | |
| | Vigilancia continua en el centro de cómputo . | ☑ | |

E = Controles existentes R = Controles recomendados.

**Tabla VI.29** Controles recomendados (Uso de los equipos).

**Controles recomendados**

***Área de:*** Información

***sub área de:*** Control de entradas/ procesos/ salidas.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Resultados incongruentes. | Revisión de la autenticidad de la información antes de ser capturada. | ☑ | |
| | Existencia de un proceso de validación de datos de entrada. | ☑ | |
| | Existencia de la documentación de los procedimientos de manejo de errores. | ☑ | |
| | Existencia de manuales, que expliquen la manera en que se introducen los datos. | ☑ | |
| | Capacitar al personal encargado de capturar la información. | ☑ | |
| b) Alteración en la integridad del procesamiento de datos . | Determinar si existen procedimientos documentados que expliquen la manera en que se procesan los datos. | ☑ | |
| | Determinar si existen controles de procesamiento para evitar errores. | ☑ | |
| | Realizar un análisis para satisfacer los requerimientos de velocidad. | ☑ | |
| c) Complejidad para interpretar los resultados. | Definir estándares para el diseño de salidas. | ☑ | |
| | Identificar los datos específicos de salida. | ☑ | |
| | Seleccionar los métodos para la presentación de la información. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.30** Controles recomendados (Control de entradas/proceso y salidas).

**Controles recomendados**

***Área de:*** Información

***sub área de:*** Acceso a la información.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Pérdida de información. | Implementar políticas de acceso a lugares donde se encuentra la información. | ☑ | |
| | Monitorear el cumplimiento de las políticas de acceso a lugares donde se encuentra la información. | | ☑ |
| | Implementar el uso de vigilancia en lugares claves. | ☑ | |
| | Capacitación al personal que está relacionado con el manejo de la información. | ☑ | |
| | Establecer turnos de trabajo. | ☑ | |
| | Hacer revisiones continuas a los sistemas de respaldo. | | ☑ |
| | Establecer una excelente capacitación al personal de sistemas de respaldo. | ☑ | |
| | Establecer una bitácora de actualizaciones de respaldo. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.31** Controles recomendados (Acceso a la Información).

| *Controles recomendados* | | | |
|---|---|---|---|
| ***Área de:*** Información<br>***Sub área de:*** Cuidado de la información. | | | |
| ***RIESGOS*** | ***CONTROLES*** | ***E*** | ***R*** |
| a) Pérdida de la información. | Existencia de un plan de contingencias. | ☑ | |
| | Existencia de equipo no "breack" | | ☑ |
| | Establecer políticas de respaldo de información. | ☑ | |
| | Calendarización para la generación de respaldos, archivos y programas. | ☑ | |
| | Hacer revisiones continuas a los sistemas de respaldo. | | ☑ |
| | Existencia de respaldos fuera del departamento de Informática | ☑ | |
| | Existencia de respaldos actualizados fuera de las instalaciones. | ☑ | |
| | Etiquetas externas de identificación a los discos, cintas y diskettes. | ☑ | |
| | Realización de pruebas con el material de respaldo. | | ☑ |
| | Accesibilidad de material de respaldo a cualquier hora. | ☑ | |
| | Capacitar a todos los usuarios para el desarrollo correcto de su trabajo. | ☑ | |
| | Auxiliar y supervisar a todos los usuarios, para tener la seguridad del desarrollo correcto de su trabajo. | ☑ | |
| | Proteger la información con claves de acceso e identificación de cada usuario. | ☑ | |
| | Detección de accesos no autorizados. | ☑ | |
| | Capacitar al personal encargado de respaldar la información. | ☑ | |

E = Controles existentes R = Controles recomendados

**Tabla VI.32** Controles recomendados (Cuidado de la Información).

***Controles recomendados***

***Área de:*** Información

***sub área de:*** Calidad de la información.

| *RIESGOS* | *CONTROLES* | *E* | *R* |
|---|---|---|---|
| a) Dificultad en la interpretación de los datos para la toma de decisiones. | Establecer procedimientos en la presentación de la información. | ☑ | |
| b) Insatisfacción del usuario. | Monitorear el grado de satisfacción del usuario en lo que se refiere a los servicios proporcionados por la función de sistemas de información. | | ☑ |

E = Controles existentes

**Tabla VI.33** Controles recomendados (Calidad de la Información).

*DEFINICIÓN DE POLÍTICAS DE SEGUIMIENTO DE USO DE CONTROLES.*

**1. ORGANIZACIÓN DEL ÁREA.**

RIESGO: A) ELECCIÓN ERRÓNEA DE LOS EQUIPOS.

- **Dar a conocer adecuadamente los objetivos de la Organización y del departamento de Informática.**

**1.- Propósito:**

Los objetivos de la Organización se deben dar a conocer al personal de Informática y a toda la Organización, los objetivos del departamento de Informática se deben de dar a conocer al personal del departamento para que no existan desviaciones de lo que se pretende obtener con el cumplimiento de los objetivos.

**2.- Lugar:**

En el departamento de Informática y los de la Organización en el departamento de Informática y en toda la Organización.

**3.- Sucesión:**

Se deben dar a conocer cuando se integra una persona a la Organización o al departamento de Informática y en recordatorio se deben difundir cada que el Director de la Organización y el Director de Informática lo consideren necesario.

**4.- Persona:**

Las personas responsables de dar a conocer los objetivos son los directivos de la Organización a los jefes de departamento para que estos a su vez los difundan con el personal que está en cada uno de los departamentos.

**5.- Medios:**

A través de documentos como : manuales, oficios , memos etc.

**6.- Cantidad:**

Cada que se considere necesario.

**2. PRESUPUESTOS/GASTOS.**

RIESGO: A) PRESUPUESTOS INSUFICIENTES.

- **El Director de Informática vigilará que se realice una buena planeación de los presupuestos y gastos.**

**1.- Propósito:**

El Director de Informática debe de supervisar que se lleve acabo una buena planeación de los presupuestos y gastos del departamento de Informática

**2.- Lugar:**

En el departamento de Informática.

**3.- Sucesión:**

Anualmente.

**4.- Persona:**

Los presupuestos deben ser realizados por el Director de Informática o por una persona capacitada a la que el Director de Informática delegue dicha actividad.

**5.- Medios:**

Basándose en presupuestos anteriores y calculando los márgenes necesarios para que estos alcancen y utilizando técnicas probadas y eficaces.

**6.- Cantidad:**

Uno anualmente.

**3. PERSONAL EXTERNO.**

RIESGO: A) RESISTENCIA A LOS CAMBIOS Y USO DE TECNOLOGÍA.

- **Definir las funciones del departamento de Informática y darlas a conocer al personal externo.**

**1.- Propósito:**

El personal externo debe conocer las funciones del personal del departamento de Informática con el propósito de que conozca el servicio que puede recibir.

**2.- Lugar:**

En cada uno de los departamentos en el que exista relación con el personal externo .

**3.- Sucesión:**

Cada que se va a proporcionar un servicio nuevo o que se modifiquen las funciones del personal de Informática.

**4.- Persona:**

El Director de Informática.

**5.- Medios:**

A través de documentos ( circulares).

## 4. PERSONAL DE INFORMÁTICA.

RIESGO: A) MAL AMBIENTE DE TRABAJO.

- **Tomar medidas para crear un buen ambiente de trabajo(buena integración y convivencia entre individuos).**

**1.- Propósito:**

El Director de Informática debe tomar medidas para que el personal de su departamento labore en un buen ambiente de trabajo; esto con el propósito de que el personal esté integrado como grupo de trabajo y la convivencia sea la adecuada.

**2.- Lugar:**

En el departamento de Informática.

**3.- Sucesión:**

Contantemente.

**4.- Persona:**

El Director de Informática

**5.- Medios:**

Propiciando buena comunicación entre el personal del departamento llevando a cabo dinámicas de grupo para integrarse como tal etc.

## DEFINICIÓN DE POLÍTICAS DE SEGUIMIENTO DE USO DE CONTROL (*SOFTWARE*)

### 1. CONTROL DE PROYECTOS

RIESGO: A) PÉRDIDA DE INFORMACIÓN Y TIEMPO A CAUSA DE ERRORES EN LOS SISTEMAS

- **Elaborar pruebas exhaustivas de todos los programas que intervienen en un sistema o que han sido modificados.**

**1.- Propósito:**

La carga de trabajo que se tiene diariamente existe una pérdida de información y tiempo cuya intención es el satisfacer las necesidades de los usuarios, sin embargo se podría realizar una ordenación de prioridades de información que conllevarían a disminuir esas pérdidas.

**2.- Lugar:**

Departamento de Informática.

**3.- Sucesión:**

La generación de información se realiza cotidianamente según sea la necesidad de las diferentes dependencias que conforman a la Organización.

**4.- Persona:**

Programadores.

**5.-Medios:**

Electrónicos.

**6.- Cantidad:**

Esta está sujeta a la demanda diaria de los diferentes departamentos de la Organización.

## 2.- ETAPAS DE DESARROLLO

A) ELABORAR UN PROYECTO DEFICIENTE.

- **Establecer adecuados canales formales de comunicación entre los empleados de la Organización.**

**1.- Propósito:**

Contar con la comunicación adecuada para adquirir la información necesaria y elaborar los sistemas, lo más apegado a las necesidades del departamento que lo solicita.

**2.- Sucesión:**

Se entablará la comunicación formal al solicitar alguna información trascendental para la adecuación y elaboración de los sistemas.

**3.- Lugar:**

En el Departamento solicitante del sistema.

**4.- Persona:**

El encargado del análisis del sistema.

**5.- Medios:**

Entrevista directa con el usuario e información formal con este.

## 3. MONITOREO DE SISTEMAS

A) SOFTWARE OBSOLETO.

- **Revisión periódica del crecimiento y desarrollo de la Organización para la adecuación de las necesidades del software.**

**1.- Propósito:**

Revisar periódicamente el software que se utiliza para la elaboración del trabajo en los departamentos y actualizar el funcionamiento de este.

**2.- Lugar:**

En todos los departamentos de la Organización que cuente sistemas implantados.

**3.- Sucesión:**

Cada que se requiera actualizar los inventarios o se vaya a realizar adquisiciones de Software, así como para llevar un correcto control al respecto.

**4.- Personal:**

Integrante del Departamento de Informática.

**5.- Medios:**

Capacitación verbal y visual de necesidades de la Organización.

**6.- Cantidad:**

Mínimo cada seis meses.

## 4. ADQUISICIÓN DE SOFTWARE

A) INCOMPATIBILIDAD DEL SOFTWARE ADQUIRIDO CON EL HARDWARE EXISTENTE.

- **Realizar una adecuada detección de necesidades y compatibilidad del software con el hardware.**

**1.- Propósito:**

Se requiere establecer un mecanismo adecuado para percibir las necesidades que se han creado en la Organización con respecto al software que se ha adquirido y que este tenga compatibilidad con el hardware existente.

**2.- Lugar:**

En el Departamento de Informática.

**3.- Sucesión:**

Se debe hacer cada que se adquiera software o se vayan a desarrollar nuevos sistemas.

**4.- Persona:**

El Director de Informática.

**5.- Medios:**

Verificando los inventarios del Hardware existente.

## DEFINICIÓN DE POLÍTICAS DE SEGUIMIENTO DEL USO DE CONTROLES (*HARDWARE*)

### 1.- ADQUISICIÓN.

RIESGO : A) ELECCIÓN ERRÓNEA DE LOS EQUIPOS.

- **Definir políticas de adquisición y rendimiento de los equipos.**

**1.- Propósito:**

Se deben de definir políticas de adquisición y rendimiento de los equipos con el propósito de no cometer errores al hacer las adquisiciones .

**2.- Lugar:**

En el departamento de Informática.

**3.- Sucesión:**

Siempre que sea necesario implantar, modificar o eliminar políticas de adquisición.

**4.- Persona:**

El Director de Informática en conjunto con el jefe de compras de la Organización.

**5.- Medios:**

A través de juntas con los directivos de la Organización y con los jefes de los departamentos involucrados en la adquisición de los equipos.

**6.- Cantidad:**

Las políticas que sean necesarias.

**2. MANTENIMIENTO.**

**RIESGO:**

A) BAJO O NULO RENDIMIENTO DE LOS EQUIPOS.

- **Contar con personal capacitado para el mantenimiento de los equipos.**

**1.- Propósito:**

Se deben de tomar medidas para que el personal encargado de dar mantenimiento a los equipos esté bien capacitado, con el propósito de que estos den el mayor rendimiento.

**2.- Lugar:**

En el departamento de Informática.

**3.- Sucesión:**

Permanentemente.

**4.- Persona:**

El Director de Informática.

**5.- Medios:**

Proporcionando capacitación al personal encargado del mantenimiento de los equipos por cursos, conferencias y talleres.

**6.- Cantidad:**

Las veces que sea necesario.

## 3. CONTROL DE FALLAS.

RIESGO: A) ACUMULACIÓN Y SOBRE CARGAS DE TRABAJO.

- **Elaboración de un plan efectivo de control de fallas.**

**1.- Propósito:**

Se debe de elaborar un plan efectivo de control de fallas con el propósito de evitar acumulación y sobrecargas de trabajo por demoras en la solución de la fallas.

**2.- Lugar:**

En el departamento de Informática.

**3.- Sucesión:**

El plan de fallas debe ser elaborado desde que se hicieron las instalaciones de los equipos.

**4.- Persona:**

El técnico de reparación de fallas.

**5.- Medios:**

La elaboración del plan de control de fallas debe ser escrito.

**4. USO DE LOS EQUIPOS.**

RIESGO: A) MALTRATO O TRATO INADECUADO DE LOS EQUIPOS.

- **Capacitar a los usuarios en el uso y funcionamiento de los equipos.**

**1.- Propósito:**

Los usuarios de los equipos deberán recibir capacitación en el uso y funcionamiento de los equipos que utilizan con el propósito de que estos no sean maltratados.

**2.- Lugar:**

En una área destinada para capacitación de personal o en los lugares donde laboran los usuarios de los equipos.

**3.- Sucesión:**

Constantemente.

**4.- Persona:**

El personal que da soporte a los usuarios.

**5.- Medios:**

A través de cursos.

## DEFINICIÓN DE POLÍTICAS DE SEGUIMIENTO DEL USO DE CONTROLES

*( Información)*

### 1. CONTROL DE ENTRADA/ PROCESOS/ SALIDAS.

RIESGO: A) RESULTADOS INCONGRUENTES.

- **Revisión de la autenticidad de la información antes de ser capturada.**

**1.- Propósito:**

Se debe revisar la autenticidad de la información antes de ser capturada con el fin de evitar resultados incongruentes.

**2.- Lugar:**

En las áreas donde se lleva a cabo la captura de la información.

**3.- Sucesión:**

Cada vez que se requiera de una entrada de datos.

**4.- Persona:**

Los capturistas de datos.

**5.- Medios:**

A través de un análisis de veracidad a los documentos y datos.

## 2. ACCESO A LA INFORMACIÓN.

RIESGO: A) PÉRDIDA DE INFORMACIÓN.

- **Implementar políticas de acceso a lugares donde se encuentra la información.**

**1.- Propósito:**

Se deben implementar políticas de acceso a lugares donde se encuentra la información para evitar la pérdida de la misma.

**2.- Lugar:**

A los lugares donde se encuentra la información.

**3.- Sucesión:**

El acceso a los lugares donde se encuentra la información debe de estar permanentemente restringido.

**4.- Persona:**

El Director de Informática.

**5.- Medios:**

Documento (Circular, folletos, memos, etc.).

**6.- Cantidad:**

Las veces que sea necesario.

## 3. CUIDADO DE LA INFORMACIÓN.

RIESGO: A) Pérdida de la información.

- **Existencia de un plan de contingencias (que acciones ejecutar cuando exista alguna catástrofe).**

**1.- Propósito:**

Se debe de contar con un plan de contingencias para evitar que los riesgos de vivir malas experiencias (las cuales pueden causar grandes daños o pérdida total de la información), se materialicen.

**2.- Lugar:**

En toda la Organización, pero sobre todo en el departamento de Informática.

**3.- Sucesión:**

Debe de existir un plan de contingencias permanentemente.

**4.- Persona:**

El Director de Informática.

**5.- Medios:**

Documento.

**6.- Cantidad:**

Un plan de contingencias.

## 4. CALIDAD DE LA INFORMACIÓN

RIESGO: A) DIFICULTAD EN LA INTERPRETACIÓN DE LOS DATOS PARA LA TOMA DE DECISIONES.

- **Establecer procedimientos en la presentación de la información.**

**1.- Propósito:**

Se deben establecer procedimientos en la presentación de la información ya que los reportes deben ser coherentes y distribuidos oportunamente a los destinatarios autorizados.

**2.- Lugar:**

En el departamento de Informática.

**3.- Sucesión:**

Cuando se haya solicitado por primera vez un formato de salida.

**4.- Persona:**

El Director de Informática.

**5.- Medios:**

En documento.

## *INFORME FINAL DE AUDITORÍA EN INFORMÁTICA.*

*Resultados obtenidos en la evaluación del área de:*

***Departamento de Informática.***

a) Descripción de la situación actual de la Organización en el área del departamento de Informática

b) Descripción detallada de:

- Problemas detectados.
- Posibles causas y problemas y fallas que originaron la situación presentada.
- Efectos que pueden tener los problemas detectados.
- Alternativas de solución.

Ensenada B.C., Abril de 1997.

Comisión Estatal de Servicios Públicos de Ensenada.
Departamento de Informática.
At'n : Coordinador de Informática
Lic. Alfonso Talavera.

Asunto: **Informe ejecutivo de Auditoría en Informática**.

Estimado Lic. Alfonso Talavera:

Por medio de la presente aprovechamos para saludarlo e informarle sobre los resultados obtenidos en la Auditoría en Informática, aplicada al centro de cómputo a su digno cargo.

En base a nuestro trabajo realizado y sustentado por las pruebas obtenidas durante la revisión de las cuatro áreas convenidas; *Departamento de Informática, Software, Hardware, e Información*, informamos a usted que la situación que guarda el centro de cómputo con respecto a su operación, seguridad, funcionamiento y uso adecuado de controles, es: ***razonablemente aceptable***, ya que no se encontraron fallas graves que afecten el funcionamiento del centro de cómputo, salvo algunos problemas importantes, controles inexistentes y otros que pueden ser mejorados, los cuales presentamos en dos anexos:

1.- Un panorama global de la situación encontrada en cada una de las áreas auditadas.
2.- Un desglose detallado de las fallas más relevantes encontradas en cada una de las áreas.

Sin más por el momento y agradeciendo la gentileza de sus atenciones, esperamos haber cumplido con sus expectativas favorablemente, quedamos de usted.

Atentamente

Ramona Estrada Sánchez
Tesista.

Noemí Montiel Herrera
Tesista.

Sonia Sánchez Espinoza.
Tesista.

**Informe del panorama global de la situación encontrada en cada una de las áreas.**

***Informe final del departamento de Informática.***

El departamento de Informática fue evaluado en cuatro sub áreas :

- Organización del área.
- Presupuestos/gastos.
- Personal externo.
- Personal de Informática.

El resultado global de la evaluación del departamento de Informática es ***aceptable,*** pero es importante resolver algunas deficiencias encontradas en las siguientes sub áreas:

La situación que presenta la ***Organización del área*** es ***deficiente,*** ya que cuenta con algunas fallas notables, como son la falta de difusión de los objetivos, deficiencia en la documentación y el monitoreo de las políticas, errores en la estructura del organigrama del departamento, la capacitación y/o actualización del personal no es constante.

Actualmente el nivel de apoyo que el departamento de Informática proporciona a la Organización, podemos calificarlo como intermedio, por que el nivel jerárquico del departamento de Informática depende de una Subdirección, el involucramiento en el proceso de planeación de la Organización es regular y el personal de Informática tiene un rol de *ejecutor* de soluciones inmediatos más que de *consultor*. Por lo que se puede considerar al departamento en un proceso de *madurez o* madurez intermedia si lo consideramos en una escala de **inicio, intermedio y maduro**.

Cabe mencionar que el departamento actualmente opera y sale adelante en el desarrollo de sus funciones, sin embargo se debe de trabajar con la mentalidad de lograr en la mayor forma posible la optimización de los servicios que el departamento proporciona a la institución para que ésta logre sus objetivos.

La situación que presenta los ***presupuestos/Gastos*** del área es ***aceptable,*** con algunas fallas como lo es el que los presupuestos no cuenten con márgenes de flexibilidad para enfrentar las contingencias que se presenten .

La situación que presenta la evaluación de ***Personal Externo*** es ***aceptable***, ya que las fallas no son graves, pero se requiere de mejorar aspectos como la comunicación entre el personal de Informática y el personal externo, la capacitación que recibe el personal externo y las condiciones ambientales en las que desarrolla su trabajo.

La situación que presenta el ***personal de Informática*** es ***aceptable,*** ya que no presenta problemas graves sin embargo hay ciertas situaciones que se deben corregir; principalmente para que no sea afectada la efectividad del personal, los problemas a corregir son la falta de motivación e incentivos para el personal de Informática, el personal se manifiesta mal remunerado.

***Informe final del Area de Software.***

El área de *SOFTWARE* fue evaluado en las siguientes sub áreas:

- Control de proyectos.
- Etapas del desarrollo de Sistemas.
- Monitoreo de Sistemas.
- Adquisición de Software.

El resultado global del área de Software es ***razonablemente aceptable,*** *pero es importante resolver algunas de las deficiencias encontradas en las siguientes sub áreas.*

La situación que presenta con respecto al ***control de proyectos*** es ***aceptable***, ya que cuenta con algunas fallas, que pueden solucionarse como lo son: la falta de definición de políticas para la realización correcta de la documentación de los sistemas (manuales).

La situación que presenta la sub área de ***etapas del desarrollo de sistemas*** es ***aceptable***, ya que cuenta con algunas fallas notables en las que se ha detectado la necesidad de que exista una buena planeación para que así, los sistemas puedan ser desarrollados óptimamente.

En este rubro encontramos que en la sub área de ***monitoreo de sistemas***, la institución opera ***aceptablemente,*** sin embargo al recurrir a la tabla de evaluación se pudo detectar que los controles expuestos en ella pueden ser mejorados si se llevan a cabo periódicamente para el desarrollo adecuado de la institución.

La situación que presenta la ***adquisición de software***, es ***aceptable*** ya que desde nuestro punto de vista se necesita atender las posibles soluciones presentadas, con la finalidad de mejorar la Organización en su conjunto.

***Informe final de los Equipos de Cómputo (Hardware).***

El área de hardware fue evaluado en cuatro sub áreas :

- Adquisición.
- Mantenimiento.
- Control de fallas .
- Uso de los equipos.

El resultado global de la evaluación del Hardware es ***aceptable,*** ya que las deficiencias encontradas no son muy graves.

La situación que presenta la evaluación de las ***adquisiciones de los equipos*** es ***aceptable***, con algunas fallas como: no actualizar y revisar periódicamente los inventarios de los equipos, no llevar acabo estudios profundos de costo - beneficio para las adquisiciones de los equipos y no tener documentadas las políticas de adquisición de los equipos en el departamento de informática.

La situación que presenta la evaluación del ***mantenimiento*** de los equipos es ***razonablemente aceptable***, ya que no se encontraron problemas muy graves sin embargo, es necesario darles solución a la menor brevedad posible para optimizar el rendimiento y funcionamiento de los equipos. Es necesario que el mantenimiento a los equipos sea ininterrumpido y se debe de contar con el número de personal adecuado.

La situación que presenta la evaluación del ***control de fallas*** de los equipos es ***deficiente,*** ya que no tiene un plan efectivo para el control de las fallas de los equipos, no se cuenta con presupuestos en los que se incluya la inversión que se requiere para las refacciones necesarias para la reparación de las fallas , las instalaciones fisicas de la red no son las óptimas, no se encuentran definidas claramente las políticas de uso y control de fallas de la red.

La situación que presenta la evaluación de ***Uso de los equipos*** es ***razonablemente aceptable,*** ya que no se cuenta con riesgos graves en el uso de los equipos, pero si existen situaciones que se deben mejorar, como son la falta de capacitación y/o actualización adecuada a los usuarios de los equipos.

***Informe final del Area de información.***

El área de información fue evaluada en 4 sub áreas:

- Control de entradas /procesos /salidas.
- Acceso a la información.
- Cuidado de la información.
- Calidad de la información.

El resultado global de la evaluación en lo referente al área de **información** es **razonablemente aceptable,** ya que no se encontraron riesgos graves que puedan afectar a la empresa, pero es importante mencionar algunos problemas detectados en las diferentes sub áreas.

La situación que presenta la evaluación de **entradas /procesos /salidas** es **aceptable,** pero se cuenta con fallas como la falta de capacitación al 100% del personal encargado de capturar la información y la no actualización de manuales, estas fallas podrían provocar en un determinado momento la dependencia de personal.

La situación que presenta la evaluación de **Acceso a la información** es **aceptable.** Recomendamos que se realicen revisiones continuas a los sistemas de respaldos así como sus respectivas pruebas de verificación, e insistimos con la capacitación al 100% para el personal que está relacionado con el manejo de la información.

La situación que presenta la **calidad de la información** es **aceptable**, recomendamos se monitorear el grado de satisfacción del usuario en lo que se refiere a los servicios proporcionados por la función de sistemas de información.

## *Informe Final de Auditoría en Informática.*

**Dirección:** Coordinador de Informática.

**Auditoría a:** Organización del área del departamento de Informática.

**Hoja No.1 De** 10

### Problemática:

Los objetivos de la *Organización* no están definidos en un documento formal y el personal de Informática no tiene conocimiento de ellos.

### Causas :

- Esta es debido a que las modificaciones administrativas se encuentran en proceso de redacción.
- El personal no conoce los objetivos de la Organización por que estos no son difundidos.

### Consecuencias :

Las consecuencia son que los objetivo de la Organización no sean cumplidos o sufran desviaciones.

### Alternativas de Solución:

Elaboran un documento en el que se especifiquen claramente los objetivos de la Organización, a un plazo de tiempo lo más corto posible , estableciendo una coordinación con los departamentos o el departamento encargado de la realización de los manuales de la Organización.

### Observaciones:

Como podemos darnos cuenta la solución de este problema no es complicada ni tampoco requiere de una inversión fuerte de dinero, simplemente se tiene que dar prioridad a las actividades que nos conduzcan al logro de los objetivos de la Organización.

## *Informe Final de Auditoría en Informática.*

**Dirección:** Coordinador de Informática.

**Auditoría a:** Organización del área del departamento de Informática.

**Hoja No.2 De** 10

**Problemática:**

Los *objetivos del departamento de Informática* no se difunden correctamente y el personal de Informática menciona no conocerlos, no recordarlos o simplemente que se enteran conforme trabajan en ellos.

**Causas :**

No se encuentran definidos en documentos y no se hacen llegar al personal de Informática.

**Consecuencias :**

Que los objetivos del departamento no sean cumplidos o sufran desviaciones y como consecuencia tampoco se cumplan los objetivos de la Organización.

**Alternativas de Solución:**

Elaborar un documento en el que se especifiquen claramente los objetivos del departamento, para que estos sean difundidos a un plazo de tiempo lo más corto posible.

**Observaciones:**

La solución a este problema es sencilla y no requiere de grandes inversiones económicas, pero el riesgo es muy grande si no tomamos conciencia de su dimensión, ya que en base a los objetivos es como se guía al departamento para realizarlos, si no se conocen se pierden y no sabe para que se está trabajando.

## *Informe Final de Auditoría en Informática.*

**Dirección:** Coordinador de Informática.

**Auditoría a:** Organización del Área del departamento de Informática.

**Hoja No.** 3 **De** 10

### Problemática:

Las *políticas del departamento de Informática* no están definidas en un documento formal.

### Causas :

Se encuentran en proceso de elaboración por el departamento que tiene la función de elaborar los manuales de la Organización.

### Consecuencias :

Son muy pocas las políticas que el personal del departamento conoce , no se pueden supervisar además de que no se cumplen correctamente.

### Alternativas de Solución:

- El Director de Informática debe solicitar al departamento de manuales de la Organización el documento correspondiente a las políticas de su departamento para que estas sean dadas a conocer y darles el seguimiento correspondiente.
- El Director de Informática redacte el documento donde se definan claramente las políticas y se las haga llegar al personal correspondiente.

### Observaciones:

Este problema se puede solucionar rápidamente y obtener resultados positivos ya que ayudará
a que el departamento funcione con más coordinación y efectividad

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a:** Organización del área del departamento de Informática.

**Hoja No.** 4 **De** 10

**Problemática:**
La ubicación del departamento de Informática dentro de la estructura organizacional no está ubicado correctamente.

**Causas :**
La ubicación que tiene actualmente el departamento de Informática es la misma desde que nació este departamento en la Organización y no ha sufrido modificaciones pues siempre a dependido de la sub dirección administrativa financiera.

**Consecuencias :**
El departamento no cuenta con la autonomía requerida para tomar las decisiones necesarias para proporcionar los servicios que se requieren para que la Organización funcione efectivamente.

**Alternativas de Solución:**
- El Director de Informática debe de promover la ubicación del departamento de Informática a un nivel staff , ya que de ésta forma obtendría mayor cobertura e independencia para operar dentro de la Organización.
- El Director debe presentar un propuesta a los directivos de la Organización donde justifique por medio de un análisis las ventajas que esto representaría para la Organización.

**Observaciones:**
La base del éxito de una empresa depende mucho de su estructura organizacional y funcional por lo que ubicar el departamento de Informática en el nivel sugerido ocasionaría mayor efectividad en las operaciones de la Organización y por supuesto del departamento de Informática, y de ésta manera poder lograr la estructura deseada para poder otorgar un perfecto funcionamiento en todas las áreas en las que está involucrada la presencia de Informática.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a:** Presupuestos/Gastos del departamento de Informática.

**Hoja No.** 5 **De** 10

**Problemática:**

La problemática encontrada en el área de Presupuestos /Gastos del departamento de Informática es que no aceptan flexibilidad en ellos.

**Causas :**

Se elaboran en base a un formato preestablecido por el departamento de presupuestos y gastos de la Organización a nivel estatal, en el cual las partidas vienen bien definidas y no se puede hacer modificaciones ni sugerencias a lo preestablecido por lo no se da oportunidad de dejar márgenes de flexibilidad por que son rechazados.

**Consecuencias :**

- Que los presupuestos sean insuficientes para cubrir los requerimientos económicos del departamento de Informática cuando se presentan contingencias.
- Que los proyectos del departamento queden inconclusos.

**Alternativas de Solución:**

- Concientizar a los ejecutivos Encargados de las finanzas de la Organización la importancia que tiene el hecho de que el departamento de Informática cuente con cierta flexibilidad en los presupuestos para solventar los gastos que se ocasiona la presencia de contingencias.
- Que el Director de Informática proponga buenos presupuestos y que estos sean bien justificados, donde defina perfectamente cada una de las partidas y demostrar beneficios de ellos.

**Observaciones:**

Dar solución a este problema seria de beneficio para la Organización ya que el departamento de Informática solucionaría las contingencias del departamento ala menor brevedad . La inversión económica de este problema es relativa ya que el Director debe presentar un buen presupuesto requerido y justificarlo de la mejor manera para que sea autorizado.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a**: Personal Externo del departamento de Informática.

**Hoja No.** 6 **De** 10

### Problemática:

El *personal externo* no conoce las funciones del departamento de Informática ni el tipo de servicio que puede recibir por parte de dicho departamento.

### Causas :

- No se difunde a los usuarios los servicios que el departamento de Informática debe proporcionar.
- No se considera necesario por que el soporte que proporciona el departamento de Informática es constante.

### Consecuencias :

- Que el personal externo desaproveche recursos de Informática en el desarrollo de su trabajo.
- Que el desempeño del trabajo del personal externo no sea muy efectivo.

### Alternativas de Solución:

- Realizar un catalogo de servicios y darlo a conocer al personal externo.
- Redactar una circular la cual contenga los servicios que el departamento de Informática proporciona y hacerla llegar al personal externo correspondiente.

### Observaciones:

Este es un problema sencillo que al resolverlo proporcionará muchos benéficos ya que el personal externo mejoraría en la eficiencia de su trabajo.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a:** Personal Externo.

**Hoja No.** 7 **De** 10

**Problemática:**

El personal externo sólo recibe la capacitación mínima necesaria en cuanto al uso y cuidado de los equipos.

**Causas :**

- No se considera necesario abundar en capacitación para el personal externo porque el departamento de Informática les proporciona soporte permanentemente.

**Consecuencias :**

- Que el personal externo sea demasiado dependiente del personal de Informática.
- Que el personal de Informática pierda demasiado tiempo atendiendo al personal externo en problemas que con un pequeño curso en grupo se solucionarían.

**Alternativas de Solución:**

- Realizar programas de capacitación y/o actualización , en los que el personal externo mejore sus conocimientos en el uso y cuidado de los equipos que opera.

**Observaciones:**

Dar capacitación al personal es la forma más viable para aumentar la efectividad de su trabajo y evitar cargas de trabajo al personal de Informática encargado de dar soporte , además no se requiere de inversiones económicas sino más bien de Organización y coordinación de los departamentos, aprovechando los conocimientos del personal de Informática y siendo este quien les otorgue los cursos de capacitación .

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a**: Personal de Informática.

**Hoja No.** 9 **De** 10

**Problemática:**

El Personal de Informática no se siente bien remunerado económicamente.

**Causas :**

- El sueldo que percibe está por debajo de sus expectativas y comparado con los sueldos perciben otros profesionistas de la misma área y en puestos similares es inferior.

**Consecuencias :**

- Esto repercute en el animo del personal de Informática y en deseos de ser mejor remunerado por el desempeño de su trabajo.
- Que el personal muestre poco interés y entusiasmo en el desempeño de su trabajo.
- Deseos de emplearse en otras empresas y por consecuencia no se crea una lealtad.

**Alternativas de Solución:**

- Promover aumentos en los sueldos del personal de Informática que satisfagan sus necesidades y expectativas económicas.
- buscar posibilidades de otorgar prestaciones.
- Remunerar con capacitación y aumentar su nivel profesional.

**Observaciones:**

La solución a estos problemas está en las manos de los sindicatos y dirección general a nivel Estado y del personal de Informática en cuanto a la promoción de aumentos que realice y tratar de otorgar otro tipo de motivaciones.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a**: Personal de Informática.

**Hoja No.** 10 **De** 10

**Problemática:**

El Personal de Informática no es capacitado y/o actualizado periódicamente para superar su nivel de desempeño de su trabajo sólo es capacitado en casos especiales y muy esporádicamente.

**Causas :**

- No hay presupuesto destinado para que el personal reciba capacitación.
- No se promueven cursos de capacitación ante la dirección de la Organización con la insistencia requerida.
- Sólo se capacita al personal que desarrolla los sistemas y requiere de un nuevo lenguaje, o en aplicaciones que se utilizaran inminentemente.
- La dirección de la Organización no es concientizada de los cambios y evoluciones que las tecnología sufre y proporciona día con día.

**Consecuencias :**

- El personal puede que exista un estancamiento en el trabajo y desempeño del personal y no evolucione de tal manera que el departamento deje de proporcionar la efectividad que de el requiere la Organización para que ésta opere correctamente.

**Alternativas de Solución:**

- Realizar programas de capacitación y actualización por medio de cursos, talleres conferencias y presentarlos a la dirección con sus respectivos análisis de costo beneficio para que estos sean aprobados y se envíe al personal de Informática a tomar dicha capacitación..

**Observaciones:**

Dar capacitación al personal es la forma más viable para aumentar la efectividad del departamento de Informática en general . Las inversiones económicas en capacitación siempre son recuperables y justificables en los resultados del trabajo del personal y beneficio para la Organización

## *Informe final de Auditoría en Informática.*

**SOFTWARE**

**Dirección:** Coordinador de Informática.
**Auditoría a:** Control de Proyectos. _ _ _

**Hoja No. 1 De. 1**

**Problemática.**
No se encuentran establecidas las políticas de documentación de los sistemas (manuales).

**Causas**
Falta de organización del departamento de Informática y coordinación con los departamentos relacionados de ésta actividad.

**Consecuencia**
No contar con la documentación necesaria para darle mantenimiento a los sistemas se puede
recurrir a pérdida de tiempo al entrar a analizar los sistemas ejecutables.

**Alternativas de solución**
Asignación de una persona para la elaboración de la documentación y/o manuales, en conjunto del programador, para evitar la pérdida de tiempo al programador.

**Observaciones.**
No se requiere de una inversión fuerte, sólo que se asigne una sola persona que esté en el departamento de Informática, para que sea el responsable de la elaboración de los documentos requeridos para el reporte de los sistemas

## *Informe final de Auditoría en Informática.*

**SOFTWARE**

**Dirección:** Coordinador de Informática.
**Auditoría a:** Etapas del Desarrollo del Sistema. _ _

**Hoja No. 1 De. 2**

**Problemática.**
Los requerimientos de solicitud de los sistemas, modificaciones a los sistemas se llevan a cabo verbalmente.

**Causa**
No se cuenta con políticas correctamente definidas para llevar a cabo las solicitudes de sistemas.
Existe desorganización y falta de organización entre los departamentos .

**Consecuencias:**
Que no se asimile correctamente el planteamiento de los requerimientos y solicitudes que presentan los usuarios.
Que se olviden las solicitudes realizadas por el usuario.
Los sistemas desarrollados no cubran los requerimientos.

**Alternativas de la solución**
Los requerimientos de nuevos sistemas o modificaciones se deben de realizar por medio de documentos escritos en los que se especifique claramente los requisitos que deben de cumplir los sistemas.
Elaborar un formato en el que se contemplen y se especifiquen cada uno de los requerimientos de los sistemas a desarrollar.

**Observaciones.**
La solución de este problema causa pequeñas inversiones en la elaboración del documento, pero es de gran beneficio, ya que los usuarios contarán con sistemas que cubran sus necesidades.

## *Informe final de Auditoría en Informática.*

**SOFTWARE**

**Dirección:** Coordinador de Informática.
**Auditoría a:** Etapas del Desarrollo del Sistema. _ _

**Hoja No. 2 De. 2**

**Problemática**
No cuenta con la elaboración e implantación de un cronograma de actividades.

**Causas**
La asignación de proyectos es verbal, lo cual provoca un gran descontrol en cuanto a los tiempos que se deben de desarrollar cada una de las etapas de los sistemas.

**Consecuencias**
No existe diferencia escrita para desarrollar otros sistemas.

**Alternativas de solución**
Realizar una planeación de actividades y establecer tiempo.

**Observación**
Los sistemas serán correctamente desarrollados en cada una de sus etapas cubriendo todas las actividades propias requeridas.

## *Informe final de Auditoría en Informática.*
## SOFTWARE

**Dirección**: Coordinador de Informática.
**Auditoría a:** Adquisición del Software. _ _

**Hoja No. 1 De. 4**

**Problemática**
No se encuentran actualizados los inventarios de software que tiene la Organización en el departamento de Informática, por lo que no se cuenta con referencia en las nuevas adquisiciones de software.

**Causas**
El departamento de Informática no lleva a cabo el control de los inventarios, pues el encargado de llevarlos es el departamento de Inventarios de la Organización.

**Consecuencias**
Invertir en software incompatible con el hardware
Invertir en software incompatible con el software
Invertir en software innecesario.

**Alternativas de solución**
Designar a una persona para que mínimo cada 6 meses actualice el inventario.

**Observaciones.**
Esta alternativa no requiere de grandes inversiones, en cambio se harán las adquisiciones correctas y necesarias en base a los requerimientos de software y de equipo.

## *Informe final de Auditoría en Informática.*

**SOFTWARE**

**Dirección:** Coordinador de Informática.
**Auditoría a:** Adquisición del Software. _ _

**Hoja No. 2 De 4**

**Problemática**
No se realiza una planeación y desarrollo adecuado de los presupuestos para que estos alcancen.

**Causas**
No se realiza un estudio de costo y tiempo que se requiere utilizar para su distribución.

**Consecuencia**:
Agotamiento del presupuesto antes de lo estimado.
Merma del presupuesto por gastos infructuosos.

**Alternativas de solución**
Realizar un estudio de tiempo y movimientos, evaluando al personal en cuanto al manejo de los recursos disponibles.
Concientizar al personal.

**Observación**
Si se concientiza al personal del buen manejo de los recursos, mayor será el beneficio en la planeación del presupuesto.

***Informe final de Auditoría en Informática.***

**SOFTWARE**

**Dirección:** Coordinador de Informática.
**Auditoría a:** Adquisición del Software. _ _

**Hoja No. 3 De. 4**

**Problemática.**
No se cuenta con un estudio en los índices inflacionario, para la prevención de alguna devaluación en los costos del software.

**Causa**
No se hace una correcta prevención para que el presupuesto no se agote antes de lo estimado.

**Consecuencias**
Al no realizarse este tipo de estudios, la Organización se puede enfrentar a una devaluación y/o alza de precios no previsto en el ejercicio presupuestal, trayendo como consecuencia la falta de adquisición de recursos necesarios, para el adecuado desarrollo organizacional.

**Alternativas de solución**
El Director de Informática deberá realizar el estudio en conjunto con el de planeación.

**Observaciones.**
El costo de este estudio no es alto, solamente se efectúa un análisis histórico, del comportamiento económico del país

*Informe final de Auditoría en Informática.*

**SOFTWARE**

**Dirección:** Coordinador de Informática.
**Auditoría a:** Adquisición del Software. _ _

**Hoja No. 4 De 4**

**Problemática:**
No se capacita adecuadamente al personal para operar el software de nueva adquisición.

**Causa**
No se cuenta con programas de capacitación el software de nueva adquisición.

**Consecuencia**
Invertir en software necesario y no utilizarlo.

**Alternativas de solución**
Proporcionar al usuario la capacitación adecuada requerida para operar el software.

**Observaciones**
Para la solución de ésta alternativa no se requiere de grandes inversiones, aún sin embargo los beneficios son mayores.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a**: Adquisición de los equipos.

**Hoja No.** 1 **De** 5

### Problemática:

Los inventarios de los equipos de cómputo no son actualizados y revisados periódicamente.

### Causas :

Los inventarios de los equipos de cómputo son actualizados y revisados hasta que el departamento encargado del control de activos fijos de la Organización los da de alta en sus inventarios.

### Consecuencias :

- Los inventarios no reflejan información veraz ni actual cada que se les consulta o revisa cuando se va a planear la adquisición de nuevos equipos.
- Se puede cometer errores al hacer adquisiciones de equipos innecesarios o no compatibles.
- No tener control sobre las garantías de los equipos.
- No controlar efectivamente la obsolescencia de los equipos.

### Alternativas de Solución:

- El Director de Informática debe tomar medidas para que los equipos sean dados de alta en los inventarios inmediatamente después de ser instalados.
- El Director puede asignar ésta tarea al personal de su departamento para que se lleve el control dentro del departamento de Informática.
- Instalar un sistemas de control de inventarios el cual maneje entradas, salidas, existencias y estado actual de los equipos.

### Observaciones:

Para solucionar este problema no se requiere de inversiones económicas muy cuantiosas, al contrario ésta medida ayudará a no hacer adquisiciones erróneas de equipos innecesarios o incompatibles.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a:** Adquisición de los equipos.

**Hoja No.** 2 **De** 5

### Problemática:

Los equipos son adquiridos en su mayoría sin hacer estudios de costo - beneficio.

### Causas :

- Las adquisiciones de los equipos se realizan tomando en cuenta la experiencia de otros centros de cómputo o por recomendaciones.
- Las adquisiciones se realizan cuando el requerimiento ya es inmediato.

### Consecuencias :

- Hacer adquisiciones apresuradas sin un estudio y análisis previo que garantice l a efectividad de l funcionamiento y rendimiento de los equipos .
- Hacer adquisiciones erróneas.
- No lograr la autorización de l presupuesto.
- No pedir el presupuesto adecuado.

### Alternativas de Solución:

- No se debe de omitir el estudio costo beneficio antes de adquirir equipos.
- Hay que llevar a cabo un análisis completo y detallado del presupuesto antes de realizar las adquisiciones de los equipos.
- Capacitar al personal en el área y realizar la presentación para que estos sean autorizados.

### Observaciones:

La solución a este problema representa un ahorro de tiempo y dinero para la institución y un mejor servicio del departamento de Informática al contar con equipos correctos en su rendimiento y funcionalidad.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a:** Mantenimiento de los equipos.

**Hoja No.** 3 **De** 5

### Problemática:

Las políticas de mantenimiento de los equipos no están definidas en documentos sin embargo se cumple con el mantenimiento de los equipos de cómputo. .

### Causas :

Se cuenta con un programa de mantenimiento en el cual van implícitas las políticas.

### Consecuencias :

- Que no sean cumplidas correctamente las políticas y se de un mal mantenimiento a los equipos.
- Las políticas se pueden perder con el paso del tiempo si no son registradas en documentos.

### Alternativas de Solución:

- Las políticas deben definirse en un manual para el mantenimiento de los equipos, y los programas de mantenimiento se deben de realizar en función del cumplimiento de las políticas no a la inversa.
- Para verificar el cumplimiento de las políticas se debe de llevar una supervisión del cumplimiento de las mismas.

### Observaciones:

Darle solución a este problema no requiere de inversiones económicas, y se obtendrá una mejor Organización y desempeño en las tareas de mantenimiento a los equipos.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a**: Control de fallas de los equipos.

**Hoja No. 4 De** 5

**Problemática:**

El control de fallas de los equipos de cómputo no se lleva acabo correctamente.

**Causas :**

- No se cuenta con un plan efectivo de control de fallas.
- El departamento no cuenta con disponibilidad de refacciones para la reparación rápida y efectiva de fallas.
- No se lleva una bitácora de las reparaciones de los equipos.

**Consecuencias :**

- No se cuenta con referencia de fallas anteriores para ser reparadas en el menor tiempo posible sino son documentadas.
- pérdida de tiempo y recursos.
- Retraso y sobre cargas en el trabajo de los sistemas y los equipos.

**Alternativas de Solución:**

- Se debe realizar un plan efectivo que prevenga y corrija adecuadamente las fallas de los equipos.
- Se recomienda que el Coordinador de Informática asigne ésta actividad a la persona que el considere adecuada, para que supervise y se le de seguimiento adecuado a dicho plan.

**Observaciones:**

Dar solución a este problema no requiere de grandes inversiones económicas, pero los beneficios serían cuantiosos ya que los equipos se repararán en un breve período de tiempo y los usuarios estarán satisfechos.

## *Informe Final de Auditoría en Informática.*

**Dirección:** de Informática.

**Auditoría a:** Control de Fallas de los Equipos.

**Hoja No.** 5 **De** 5

**Problemática:**

Las políticas de uso y de control de fallas de la red no están documentadas en un manual .

**Causas :**

- Se difunden verbalmente .
- No se cuenta con las políticas suficientes disponibles en documentos para que las fallas de la red sean controladas efectivamente .

**Consecuencias :**

- La red está más susceptible a fallas sino se cuenta con políticas de control de las fallas.
- Las fallas no podrán ser reparadas en base cumpliendo con las políticas de control de fallas sino se encuentra personal que conozca las políticas ya que estas no están documentadas.
- El departamento debe de estar bien organizado y contar con las políticas necesarias y correctamente definidas.

**Alternativas de Solución:**

- Las políticas de control de fallas deben ser definidas en un documento y estar a disposición de quienes deben ser los encargados de llevarlas a cabo .
- El departamento debe de estar bien organizado y contar con las políticas necesarias y correctamente definidas.

**Observaciones:**

Para que las funciones o tareas se realicen correctamente es más factible que es ten documentadas y así darles un mejor seguimiento y los políticas para el mantenimiento de los equipos no son una excepción, además no se requiere de inversiones económicas y se obtendrán grandes beneficios en cuanto al funcionamiento de los equipos de cómputo.

## *Informe Final de Auditoría en Informática.*

**INFORMACIÓN**

**Dirección:** de Informática .

**Auditoría a:** Control de Entradas /Procesos /Salidas de información.

**Hoja No.** 1 **De** 5

### Problemática:

Los manuales para consulta de los usuarios que explican la manera en que se introducen los datos, con el fin de evitar posibles errores, no se encuentran actualizados.

### Causas :

El personal de Informática cuenta con sobrecargas de trabajo.

### Consecuencias :

Provoca un margen más grande de error.

### Alternativas de Solución:

Actualizar los manuales cada vez que se exista una modificación al sistema.

### Observaciones:

La actualización de los manuales no requiere de mucho tiempo, sin embargo los beneficios de las consultas a los manuales que realice el usuario, se reducirán aún más los errores en la entrada de datos, pero sobre todo minimiza la dependencia de personal. (Personal clave)

## *Informe Final de Auditoría en Informática.*

**INFORMACIÓN**

**Dirección:** de Informática .

**Auditoría a:** Control de Entradas /Procesos /Salidas de información.

**Hoja No. 2 De 5**

**Problemática:**
El personal encargado de capturar la información, recibe la capacitación mínima necesaria para operar los sistemas.

**Causas :**
Se considera que no se requiere una capacitación completa, ya que se cuenta con soporte técnico permanente.

**Consecuencias :**
Esto origina que se ocupe demasiado tiempo en dar asesorías.

**Alternativas de Solución:**
Capacitar al 100% al personal encargado de capturar la información, con el fin de que desarrolle correctamente su trabajo.

**Observaciones:**
Este problema es sencillo de resolver y no requiere de inversión económica, beneficiándose entonces, en evitar aún más un margen de error, pero sobre todo minimiza la dependencia de personal clave.

## *Informe Final de Auditoría en Informática.*

**INFORMACIÓN**

**Dirección:** de Informática .

**Auditoría a**: Control de Entradas /Procesos /Salidas de información.

**Hoja No.** 3 **De** 5

### Problemática:

Los procedimientos que explican la manera en que se procesan los datos no están actualizados.

### Causas:

El Director de Informática no lo considera relevante

### Consecuencias :

En caso que se lleguen a interrumpir los procesos o sufran alguna alteración en su integridad, no se cuenta con referencias documentadas para poder solucionar el problema con rapidez.

### Alternativas de Solución:

Actualizar los procedimientos que explican la manera en que se procesan los datos.
Se debe de contar con un manual por sistema que incluya todos los procedimientos del sistema.

### Observaciones:

Esta solución no provoca gasto alguno, en cambio los beneficios recibidos son grandes, como minimizar la dependencia de personal, el factor tiempo en consultas o en caso de alguna interrupción en el procesamiento de los datos. La seguridad que se le de a la información, depende en gran medida la operación de la Organización.

## *Informe Final de Auditoría en Informática.*

**INFORMACIÓN**

**Dirección:** de Informática .

**Auditoría a**: Cuidado de la información.

**Hoja No.** 4 **De** 5

**Problemática:**
No se realizan revisiones, ni realización de pruebas a los sistemas de respaldo.

**Causas :**
El Director de Informática no lo considera relevante.

**Consecuencias :**
La información puede sufrir daños y/o pérdida total.

**Alternativas de Solución:**
Realizar revisiones continuas y pruebas a los sistemas de respaldo, por lo menos una vez a la semana, apoyándose en una bitácora como medio de control.

**Observaciones:**
Esta solución no provoca gasto alguno, en cambio los beneficios recibidos son grandes, pues de la seguridad que se le de a la información, depende en gran medida la operación de la Organización.

## *Informe Final de Auditoría en Informática.*

**INFORMACIÓN**

**Dirección:** de Informática .

**Auditoría a:** Calidad de la información.

**Hoja No.** 5 **De** 5

### Problemática:

El departamento de Informática no monitorea el grado de satisfacción de los usuarios en lo que se refiere a los servicios proporcionados por la función de sistemas de información.

### Causas :

El departamento de Informática ocupa su mayor tiempo en darles solución a los requerimientos y problemas que surgen en la red, provocando con esto el descuido de otras funciones.

### Consecuencias :

La insatisfacción del usuario por los servicios proporcionados, está reflejada en la calidad de la
información.

### Alternativas de Solución:

Monitorear el grado de satisfacción del usuario en lo que se refiere a los servicios proporcionados por la función de sistemas de información.

### Observaciones:

Esta solución no requiere de inversión económica, originando en cambio grandes beneficios para el departamento de Informática y los usuarios.

# CAPÍTULO VII
# CONCLUSIONES GENERALES.

## 1. Inexistencia de metodologías prácticas para la aplicación de Auditorías en Informática.

Después de haber realizado el estudio de diferentes metodologías podemos concluir que actualmente es muy difícil encontrar metodologías prácticas que proporcionen los elementos necesarios para la aplicación de Auditorías en Informática efectivas y rápidas, puesto que las encontradas por lo general son complejas y tardadas, además, la mayoría de las metodologías son ediciones de otros países (especialmente U.S.A.), por lo que resulta más complicado hacer una interpretación clara de las etapas, fases y tareas de las mismas, no tanto por el idioma sino que la interpretación de los procedimientos para la aplicación de las auditorías están enfocados a ambientes de trabajo distintos.

Las metodologías deben estar orientadas, como su nombre lo indica, a ser un método ordenado para guiar paso a paso y de manera práctica a los profesionistas interesados a evaluar y revisar los diferentes aspectos de la Informática.

## 2.- Desaprovechamiento de la Auditoría en Informática por la mayoría de las Organizaciones.

En base a las investigaciones realizadas con respecto a la Auditoría en Informática, podemos concluir que en la mayoría de las Organizaciones no se tiene conocimiento del grado de apoyo que la Auditoría en Informática representa en la misma, ya que actualmente no se difunde lo necesario o apenas empieza a difundirse. La mayoría de las organizaciones creen que es necesario proteger la información que se maneja con recursos tecnológicos más no por ello, están dispuestos a invertir dinero, tiempo y compromiso para eliminar sus problemas del manejo, cuidado, seguridad y control de sus recursos de informática.

También es importante señalar que aunque son muy pocas las empresas en nuestro país que utilizan la Auditoría en Informática, éstas lo hacen correctamente ya que en México existen profesionistas con mucha experiencia y conocimiento del área de Auditoría en Informática, sólo que como lo mencionamos anteriormente, este tópico no tiene la demanda que merece.

Actualmente la Auditoría en informática se lleva a cabo en organizaciones muy grandes como en el sector bancario, grandes industrias, empresas de comunicaciones (las cuales utilizan tecnología de punta) en empresas transnacionales y muy poco en empresas medianas.

**3.- Resultados obtenidos al implantar nuestra guía práctica.**

La guía práctica para la aplicación de Auditorías en Informática se implantó en el centro de cómputo de la C.E.S.P.E. con la finalidad de probarla y proponerla como un proceso metodológico que nos llevó a obtener un informe profesional de la situación que presenta dicho centro de cómputo en el desempeño de la función de Informática, el cual obtuvimos de manera satisfactoria.

El ambiente en el que se desarrolló la Auditoría con respecto al personal del departamento de Informática fue de cooperación e interés por algunas personas ya que mencionaron que les gustaría mejorar el desempeño de su trabajo y del departamento en general. Con relación a los usuarios, el ambiente fue distinto ya que podemos concluir que les hace falta mucha capacitación e información general de lo que representa para ellos la función de informática con respecto a su propio trabajo, así como, ser motivados a tener un poco más de curiosidad o interés en tratar de mejorar la calidad de su trabajo, no por que consideremos que lo hacen mal, lo mencionamos porque al presentarles los test que utilizamos para recopilar información sentimos que lo consideraron solamente como una carga más de trabajo.

Aún cuando sabían que esa información serviría para mejorar su trabajo e incluso el servicio que el departamento de Informática les proporciona como usuarios. Por esta situación recomendamos que si la implantación de la guía práctica se aplica en Instituciones Gubernamentales, se lleve a cabo otro tipo de recopilación de información, por ejemplo visual, entrevistas etc.

**4.- conclusión final.**

El haber desarrollado una guía práctica para la aplicación de auditorias en Informática, ha sido una labor muy productiva ya que ésta tarea no llevo a realizar varias investigaciones, además de cuestionamientos, de los que aprendimos muchos aspectos de nuestra carrera de Lic. en Informática que no habíamos asimilado o enfocado en la forma en que hoy gracias a todas las experiencias obtenidas las visualizamos. Sabemos que la guía se puede mejorar en algunas de sus etapas y nos gustaría que esto no fuera la conclusión de un trabajo, sino el inicio de otros más, de quienes la utilicen, para que se llegue a convertir en una metodología formal, probada y aprobada por los profesionistas que la utilicen en la aplicación de sus Auditorías en Informática.

# Bibliografía:


- Análisis y diseño de sistemas de información. Senn James A. Mc Graw Hill.
- Organización, Guía para problemas y práctica. Jhon Shiid. C E C S A.
- Sistemas de Información Basados en computadoras para la administración moderna. Robert g. Murdick , Joel E. Ross. Editorial Diana.
- Administración contemporánea. David R. Hampton. Mc Gril Hill.
- Sistemas de Información Teoría y Práctica. John G. Burch Jr., Felix R. Strator Jr.
- Auditoría en Informática.( Enfoque metodológico) Enrique Hernández Hernández. CECSA
- Auditoría en Centros de Cómputo (objetivos, lineamientos y procedimientos). David H. Li. Editorial Trillas.
- Seguridad en Centros de Cómputo. ( Políticas y Procedimientos). Leonardo H. Fine.

- Auditoría en Informática . José Antonio Echenique García. Editorial MC Grey Hill.
- Auditoría en Informática. Diplomado Kernel Módulos 1,2,3,5,6.
- Métodos de Investigación por Encuesta, Earl R. Babbie. 1988 FOTOEDISA.
- El presupuesto. Cristóbal del Río González. ECASA.
- Administración de Empresas. Reyes Ponce Agustín., LIMUSA.
- Sistemas de Información Administrativa. Segunda Edición 1993., Prentice-Hall Hispanoamericana, S.A. E.U.A.
- Conceptos de los Sistemas de Información para la Administración. Lucas Henry C. Jr.

## ANEXO A.

Este anexo tiene la finalidad de proporcionar herramientas y técnicas, que agilicen la recopilación de información en el desarrollo de las fases de la guía práctica que proponemos en el capitulo V e implantamos en el caso práctico desarrollado en el capítulo VI.

## DOCUMENTACIÓN, ESTREVISTAS, Y OBSERVACIONES FACTIBLES DE LAS DIFERENTES ÁREAS A AUDITAR.

### ÁREA DEL DEPARTAMENTO DE INFORMÁTICA

**Documentación requerida.**

**A nivel organizacional:**

1.- Manual de la Organización cuyo contenido mínimo será:
- Organigrama con jerarquías.
- Funciones de la Organización.
- Objetivos y políticas.
- Análisis y descripción de puestos.
- Historia y antecedentes.
- Manual de normas.

2.- Objetivos de la dirección (corto, mediano, largo plazo).
3.- Políticas y Normas de la dirección.

**A nivel del departamento de informática:**

1.- Organigrama del departamento.
2.- Objetivos del departamento (corto, mediano, largo plazo)
3.- Políticas del departamento.
4.- Número de personas y puestos en el departamento.
5.- Políticas y procedimientos de contratación del personal.
6.- Reglamento interno.
7.- Presupuestos y costos del departamento.
8.- Programa de capacitación (Vigente y capacitación dada el último año).

**Entrevista al Director de Informática.**

**Preguntas:**

1.- ¿ La estructura actual del departamento está encaminada al logro eficiente de los objetivos?
2.- ¿ Están definidos y establecidos en un documento los objetivos del departamento?
3.- ¿ Quién define los objetivos?
4.- ¿ Cómo se difunden los objetivos?
5.- ¿ El personal del departamento conoce los objetivos?
6.- ¿ El Director de Informática tiene buena comunicación con superiores e inferiores de la Organización ?
7.- ¿ Considera adecuada la estructura actual de la Organización ?
8.- ¿ Considera adecuada la estructura actual del departamento de Informática?
9.- ¿ Considera que el número de personal que actualmente conforma el departamento es el adecuado?
10.- ¿ De que manera se planea el trabajo del departamento?
11.- ¿ Considera que su autoridad va de acuerdo a su responsabilidad?
12.- ¿ En su departamento se han presentado conflictos por autoridad?
13.- ¿ Existe algún sistema de sugerencias y quejas hacia al personal del departamento?
14 .- ¿ Las funciones del departamento están definidas en algún documento?
15.- ¿ Cual es la forma de dar a conocer las funciones?
16.- ¿ El departamento participa en la formulación de las funciones?.
17.- ¿ Conocen los demás departamentos o áreas las funciones de informática?
18.- ¿ Se cumplen los objetivos del departamento?
19.- ¿ Se elabora algún reporte sobre el grado de avance en el cumplimiento de los objetivos?
20.- ¿ Con qué frecuencia se realiza este reporte y hacia quien va dirigido?
21.- ¿ Se realizan actualizaciones de los objetivos?
22.- ¿ Cuándo fue la ultima revisión y actualización de los objetivos?
23.- ¿ El departamento cuenta con un presupuesto anual?
24.- ¿ Quiénes formulan es presupuesto?
25.- ¿ Usted participa directamente en la elaboración de los presupuestos y gastos anuales?

**Entrevista al personal de Informática.**

**Preguntas:**

1.- ¿ Puesto que desempeña?
2.- ¿ Describa las actividades propias de su puesto? (Diarias, periódicas, eventuales).
3.- ¿ Conoce los objetivos del departamento?
4.- ¿ Me puede mencionar los objetivos?
5.- ¿ Conoce las políticas del departamento?
6.- ¿ Me puede mencionar las políticas?
7.- ¿ Cómo se deciden y definen las políticas que se implantan?
8.- ¿ Cuáles políticas se tienen establecidas para su puesto?
9.- ¿ Cómo calificaría Ud. el ambiente de trabajo en que se vive en el departamento?
10.- ¿ Se siente motivada para desempeñar adecuadamente su trabajo?
11.- ¿ Cómo se estimula y recompensa al personal de su departamento?
12.- ¿ Existen oportunidades de ascensos y promociones?
13.- ¿ Ha participado en programas de capacitación en el último año?
14.- ¿ Qué tipo de capacitación es la que ha recibido?
15.- ¿ Evalúan al personal después de haber recibido capacitación?
16.- ¿ Cómo se lleva a cabo la supervisión del trabajo en su departamento?
17.- ¿ Existen factores internos que limiten el buen desempeño de su trabajo?
18.- ¿ Conoce el reglamento interno de trabajo de su departamento?
19.- ¿ Se siente adecuadamente remunerado?

**Entrevista a los usuarios.**

**Preguntas:**

1.- ¿ Considera que el número de personal que labora en el departamento de informática es el adecuado?
2.- ¿ Es frecuente la repetición de los trabajos encomendados el personal de informática.
3.- ¿ El personal de informática es discreto con el manejo de información confidencial?
4.- ¿ Existen políticas conocidas para proporcionar los servicios de informática?
5.- ¿ Considera que el personal de informática para brindarle un buen servicio a Ud. como usuario?
6.- ¿ Ud. aporta al personal de informática sugerencias para mejorar el desempeño de su trabajo?
7.- ¿ Qué tratamiento se les da a sus sugerencias?
8.- ¿ Ud. se siente capacitado para realizar sus tareas a lo gustaría recibir capacitación?
9.- ¿ Qué temas le gustarían para que lo capacitaran?

# ÁREA DE SOFTWARE

**Documentación requerida.**

1.- Políticas de documentación de sistemas.
2.- Políticas de mantenimiento de sistemas.
3.- Políticas de desarrollo de sistemas.
4.- Políticas de uso de antivirus.
5.- Estándares de análisis y diseño de sistemas.
6.- Manual de usuario, del programador y técnico.
7.- Inventario de software del departamento de Informática.

**Entrevista al Director de Informática.**

**Preguntas:**
1.- ¿ Cómo se asignan los proyectos?
2.- ¿ Cómo se define la realización de un proyecto?
3.- ¿ Se tiene definido al personal que va a desarrollar los proyectos?
4.- ¿ Se cuenta con metodologías de desarrollo de proyectos?
5.- ¿ Documentan los sistemas?
6.- ¿ Existen Métodos de pruebas e implantación?
7.- ¿ Cuentan con una bitácora de implantación de sistemas?

**Encuesta al personal de Informática.**

**Preguntas:**
1.- ¿ Qué tipo de software se utiliza?
2.- ¿ El software es monousuario o multiusuario?
3.- ¿ Si el software es multiusuario, para cuantos usuarios es?
4.- ¿ Versiones del Software?
5.- ¿ Plataformas en las que funcionan?
6.- ¿ Sistemas operativos que utilizan y los que se pueden utilizar?
7.- ¿ Requerimientos mínimos para el funcionamiento, tanto básicos como ideales?
8.- ¿ Qué herramientas de programación utilizan?
9.- ¿ Qué herramientas de comunicación utilizan?
10.- ¿ Qué herramientas administrativo contables utilizan?

11.- ¿ Utilerias que se utilizan?
12.- ¿ Descripción y características de cada uno de los programas que se utilizan?
13.- ¿ Porcentaje en el que son utilizados?
14.- ¿ En qué fechas fueron instalados los sistemas?

**Encuesta a los usuarios.**

¿ Los sistemas de cómputo utilizado en su departamento satisfacen sus necesidades de trabajo (tiempo/funciones) ?

¿ Cuando ha requerido un sistema y/o modificación de éstos, se les han proporcionado puntualmente por el departamento de informática?

¿ La atención que recibe del personal que labora en el departamento de informática con respecto al software es:

¿ Tiene usted un manual de usuarios pos sistema?

¿ Es claro el manual del usuario?

¿ Ha participado en el diseño del sistema de información y que hace?

¿ Por la naturaleza de su trabajo e información que genera, considera necesario la creación de un sistema de cómputo, especifico para el procesamiento de la misma ?.

## ÁREA DE HARDWARE

**Documentación requerida.**

1.- ¿ Documentación sobre los equipos, número de ellos localización y características de los instalados y por instalar?
2.- ¿ Estudio de viabilidad de los equipos?
3.- ¿ Fechas de instalación de los equipos?
4.- ¿ Contratos vigentes de compras, renta y servicios de mantenimiento?
5.- ¿ Contratos de seguros?
6.- ¿ Configuración de los equipos, capacidades actuales y máximas?
7.- ¿ Planes de expansión?
8.- ¿ Políticas de operación y uso de los equipos?
9.- ¿ Inventario actual de los equipos?
10.- ¿ Mapa del centro de cómputo?

**Entrevista al Director de Informática.**

**Preguntas:**
1.- ¿ Quién realiza los estudios de viabilidad de los equipos?
2.- ¿ Quién elabora las políticas de uso para los equipos?
3.- ¿ Cada cuando se actualizan las inventarios de los equipos?
4.- ¿ Quién realiza los análisis de COSTO-BENEFICIO para la adquisición de los mismos?
5.- ¿ Considera que el departamento tiene una buena ubicación en la organización?
6.- ¿ Han tenido problemas por la ubicación de los equipos?
7.- ¿ Existe un programa de mantenimiento de los equipos?
8.- ¿ Cada cuando se le da mantenimiento a los equipos?
9.- ¿ Se lleva un registro del mantenimiento proporcionado?
10.- ¿ Cuentan con normas de seguridad para el acceso a los equipos?
11.- ¿ Quién vigila que estas normas se cumplan?
12.- ¿ Cómo protegen el equipo de desastres naturales?
13.- ¿ Cómo protegen los equipos del desgaste natural por el paso del tiempo?
14.- ¿ Se monitorea constantemente el correcto uso de los equipos por parte de los usuarios?
15.- ¿ Se lleva acabo un control actualizado de las fallas de los equipos?
16.- ¿ Existe un programa preventivo de fallas?
17.- ¿ Con qué disponibilidad de refacciones cuentas?

**Entrevista a los usuarios de los equipos.**

**Preguntas:**

1.- ¿ Para utilizar su equipo de computo, Ud. cuenta con clave de acceso?
2.- ¿ El equipo de computo que Ud. utiliza funciona correctamente?
3.- ¿ El equipo que utiliza, lo comparte con otras personas?
4.- ¿ Ha detectado lentitud en su computadora al realizar su trabajo?
5.- ¿ Cuando su equipo de computo presenta fallas, el tiempo de respuesta por parte del depto. de Informática es aceptable?
6.- ¿ El tiempo de solución de fallas de su equipo por parte del depto. de Informática como es?
7.- ¿ Cómo desempeña su trabajo, cuando su equipo de computo esta siendo reparado?
8.- ¿ Cómo considera Ud. el equipo que utiliza para el desempeño de su trabajo?
9.- ¿ Cual es la actitud del personal de Informática, al solicitarles algún servicio en cuanto a la reparación de fallas de los equipos de computo?
10.-¿ En GENERAL como considera Ud. El servicio proporcionado con respecto al equipo de cómputo?

# ÁREA DE INFORMACIÓN

**Documentación requerida.**

1.- Manuales que expliquen la manera en que se introducen los datos.
2.- Manuales que expliquen la manera en que se procesan los datos.
3.- Controles de procesamiento documentados para evitar errores.
4.- Estándares definidos para la presentación de la información.
5.- Métodos específicos para la presentación de la información.
6.- Documento de diseño de salidas.
7.- Políticas de acceso documentadas.
8.- Planes de contingencias contra perdida de Información.
9.- Bitácora de actualizaciones de respaldo.
10.- Calendarización en la generación de respaldos.

**Entrevista al Director de Informática.**

**Preguntas:**

1.- ¿ Cómo se supervisa que la información haya sido bien capturada?
2.- ¿ Cómo se supervisa que la información haya sido totalmente capturada?
3.- ¿ Se capacita al personal para la captura de información?
4.- ¿ Se cuenta con controles de procesamiento para evitar errores?
5.- ¿ Existen controles de procesamiento como:
   - Investigar cualquier desviación del operador con respecto a los procedimientos establecidos
   - Uso de contadores de lotes de datos procesados
   - Uso de contadores de registro de datos procesados
   - Uso de totales de control de datos procesados?
6.- ¿ Existen controles de procesamiento para evitar caídas del sistema?
7.- ¿ El procesamiento de los datos satisface los requerimientos de velocidad?
8.- ¿ Se cuenta con políticas de acceso en lugares donde se encuentra la información?
9.- ¿ Se monitorea el cumplimiento de éstas políticas?
10.-¿ Se cuenta con vigilancia en lugares claves?
11.-¿ Se le da capacitación al personal que está relacionado con el manejo de la Información?
12.- ¿ De que manera se llevan a cabo los equipos de trabajo en cuanto al horario, por seguridad de la información ?

13.- ¿ Se cuenta con un sistema de respaldo para la información?
14.- ¿ Se realizan revisiones continuas a los sistemas de respaldo?
15.- ¿ Cada que tanto tiempo se hacen revisiones a los sistemas de respaldo?
16.- ¿ Se tienen responsables del resguardo de la información?
17.- ¿ Quién realiza los respaldos?
18.- ¿ Se capacita al personal encargado de respaldar?
19.- ¿ Cada cuanto tiempo se hacen los respaldos?
20.- ¿ Se cuenta con una bitácora de actualizaciones de respaldos?
21.- ¿ Se cuenta con planes de contingencias contra perdida de información?
22.- ¿ Se cuenta con equipo "no breack" (sistema de energía ininterrumpida)
23.- ¿ Se lleva una calendarización en la generación de respaldos, archivos y programas?
24.- ¿ Se cuenta con respaldos actualizados fuera del departamento de Informática?
25.- ¿ Se cuenta con respaldos actualizados fuera de las instalaciones?
26.- ¿ Se identifican los discos, cintas y diskettes con etiquetas externas?
27.- ¿ Se realizan pruebas con el material de respaldo ?
28.- ¿ Se puede accesar el material de respaldo a cualquier hora?
29.- ¿ Se supervisa a todos los usuarios después de la capacitación, para tener la seguridad del desarrollo correcto de su trabajo ?
30.- ¿ Con qué sistema de acceso se protege la información?
31.- ¿ Cómo se detectan los accesos no autorizados?
32.- ¿ Se cuenta con políticas de ubicación del equipo de cómputo?
33.- ¿ Es adecuada la presentación de reportes generados por los sistemas?

**Entrevista al encargado de Sistemas**

**Preguntas:**

1.- ¿ Existe algún proceso de validación de datos de entrada?
2.- ¿ Existen procedimientos documentados <manuales> que expliquen la manera en que se introducen los datos ?
3.- ¿ Existen procedimientos documentados <manuales > que expliquen la manera en que se procesan los datos ?
4.- ¿ Qué tipo de controles de procesamiento se cuenta para evitar errores?
5.- ¿ Existe documentación de procedimientos para el manejo de errores?
6.- Pedir procedimientos formales que se deban observar antes de que sean aceptadas las salidas del sistema.
7.- ¿ Se cuenta con planes de contingencias contra perdida de información?
8.- ¿ Se cuenta con equipo "no breack" (sistema de energía ininterrumpida)
9.- ¿ Se realizan revisiones continuas a los sistemas de respaldo?
10.- Se lleva una calendarización en la generación de respaldos, archivos y programas?

11.- ¿ Se cuenta con respaldos actualizados fuera del departamento de Informática?
12.- ¿ Se cuenta con respaldos actualizados fuera de las instalaciones?
13.- ¿ Se identifican los discos, cintas y diskettes con etiquetas externas?
14.- ¿ Se realizan pruebas con el material de respaldo?
15.- ¿ Se puede accesar el material de respaldo a cualquier hora?
16.- ¿ Se supervisa a todos los usuarios después de la capacitación, para tener la seguridad del desarrollo correcto de su trabajo ?
17.- ¿ Con qué sistema de acceso se protege la información?
18.- ¿ Cómo se detectan los accesos no autorizados?
19.- ¿ Se cuenta con políticas de ubicación del equipo de cómputo?
20.- ¿ Se capacita al personal encargado de respaldar?
21.- ¿ Es adecuada la presentación de reportes generados por los sistemas?

**Entrevista al usuario.**

**Preguntas:**

1.- ¿ Tiene usted a su alcance los manuales que explican la manera en que se introducen los datos ?
2.- ¿ Se le capacita a usted antes de empezar a capturar en un nuevo sistema?
3.- ¿ Está satisfecho con la velocidad de respuesta del sistema en el que usted está operando?
4.- ¿ Considera que los resultados que le proporciona el sistema que está usted operando son de entera satisfacción ?
5.- ¿ Es adecuada la presentación de reportes generados por el sistema que usted maneja?
6.- ¿ Cómo considera usted, en general el servicio proporcionado por el departamento de Informática ?

**Observaciones.**

1.- Observar la velocidad de respuesta de los sistemas.
2.- Existencia de medidas de seguridad vs. sustracción de información confidencial.
3.- Claves de acceso para ingresar a los sistemas.
4.- Observar la facilidad de acceso en donde se encuentran los controles.
5.- Observar el equipo de energía ininterrumpida.
6.- Ubicación física de los respaldos de la información.
7.- Etiquetas de identificación a los discos, cintas y diskettes.
8.- Ubicación física del equipo.

# TESTS SUGERIDOS PARA LA RECOPILACIÓN DE LA INFORMACIÓN DE LAS DIFERENTES ÁREAS.

## *TEST PARA LA EVALUACIÓN DE PERSONAL*

*1.- Considera que el número de personas que laboran en el departamento de Informática para otorgar un buen servicio o apoyo es:*
*Insuficiente [ ] Aceptable [ ] Suficiente [ ] indicado [ ] Excesivo [ ]*

*2.- ¿ Es frecuente la repetición de un trabajo encomendado al departamento de Informática?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*3.- ¿ El personal de informática es discreto en el manejo de información confidencial?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*4.- ¿ Existen políticas conocidas para proporcionarle servicios por parte del departamento de Informática ?*
*Si [ ] No [ ]*

*5.- ¿ En general, acata el personal de informática las políticas, sistemas y procedimientos establecidos?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*6.- ¿ Considera que el personal de informática está capacitado para brindarle un buen servicio a usted ?*
*Si [ ] No [ ]*
*¿Por qué?*_____.

*7.- ¿ Ud. Aporta al depto. de informática sugerencias para mejorar el desempeño de su trabajo?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*8.- ¿ Las sugerencias que usted aporta son tomadas en cuenta?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*9.- ¿ Qué tratamiento se le da a sus sugerencias?*_____
_____

*10.- ¿ El trabajo del personal de informática según su apreciación personal es de calidad:*
*Deficiente [ ] Regular [ ] Aceptable [ ] Buena [ ] Excelente [ ]*

## *TEST PARA LA EVALUACIÓN DE LOS EQUIPOS DE CÓMPUTO*

*1.- ¿ Para utilizar su equipo de cómputo, Ud. cuenta con clave de acceso?*
*Nunca [ ] Rara vez [. ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*2.- ¿ El equipo de cómputo que Ud. utiliza funciona correctamente?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*3.- ¿ El equipo que utiliza, lo comparte con otras personas ?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*
*Con cuantas personas:_____.*

*4.- ¿ Ha detectado lentitud en su computadora al realizar su trabajo?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*

*5.- ¿ Cuándo su equipo de cómputo presenta fallas, el tiempo de respuesta por parte del departamento de Informática es:*
*Excesivo [ ] Tardado [ ] Aceptable [ ] Satisfactorio [ ] Inmediato [ ]*

*6.- El tiempo de Solución de fallas de su equipo por parte del departamento. de Informática*
*Es: Excesivo [ ] Tardado [ ] Aceptable [ ] Satisfactorio [ ] Inmediato [ ]*

*7.- ¿ Cómo desempeña su trabajo, cuando su equipo de cómputo esta siendo reparado?*
*No lo realiza [ ] Le proporcionan otro [ ] Manualmente [ ] Se acumula [ ]*

*8.- Considera Ud. que el equipo que utiliza para el desempeño de su trabajo es :*
*Inadecuado [ ] obsoleto [ ] demasiado moderno [ ] indicado [ ]*
*¿Por qué ?*
_____

*9.- ¿ Cuál es la actitud del personal de Informática, al solicitarles algún servicio en cuanto a la reparación de fallas de los equipos de computo?*
*Negativa [ ] Indiferente [ ] Accesible [ ] Buena [ ] Excelente [ ]*

*10.- ¿ En GENERAL como considera Ud., el servicio proporcionado por el dpto. de Informática con respecto al equipo de cómputo?*
*Pésimo [ ] Deficiente [ ] Aceptable [ ] Bueno [ ] Muy bueno [ ]*

## *TEST PARA LA EVALUACIÓN DEL SOFTWARE.*

*1.- ¿ Los sistemas de cómputo utilizados en su departamento, satisfacen sus necesidades de trabajo ? (en tiempo).*
*Lento [ ] Tardado [ ] Aceptable [ ] Satisfactorio [ ] Inmediato [ ]*
*¿Por qué?* _____

*2.- ¿ Cuando ha requerido un sistema de cómputo nuevo o modificación a uno existente se le ha proporcionado puntualmente por el departamento de Informática?*
*Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre [ ]*
*¿Por que?* _____

*3.- ¿ Tiene Ud. un manual de usuarios por cada sistema de cómputo que maneja?*
*Si [ ] No [ ]*

*4.- ¿ Es claro el manual del usuario?*
*Si [ ] No [ ]*

*5.- ¿ Ha participado en el diseño de Sistemas de cómputo que usted utiliza?*
*Si [ ] No [ ]*
*¿De qué forma?* _____

*6.- ¿ Por la naturaleza de su trabajo e información que genera, considera necesario la creación de algún sistema de cómputo específico?*
*Si [ ] No [ ]*
*¿Cúal?* _____

*7.- La atención que recibe del personal que labora en el dpto. de Informática con respecto al sistema de cómputo es:*
*Deficiente [ ] Aceptable [ ] Satisfactorio [ ] Buena [ ] Excelente [ ]*
*¿Porque?*

## *TEST PARA LA EVALUACIÓN DE LA INFORMACIÓN*

### *EVALUACIÓN DEL FLUJO DE LA INFORMACIÓN*

*1.- ¿ Se le entregan con puntualidad la información <documentos, trabajos > provenientes de otros departamentos de la empresa ?*
*[ ] Nunca [ ] Rara vez [ ] Ocasionalmente [ ] Generalmente [ ] Siempre*

*2.- ¿ Qué procesos y /o documentos realiza usted manualmente?*
_____
_____
_____

*3.- ¿ Qué reportes <documentos > entrega usted y a quién?*
_____
_____

*4.- ¿ En qué forma los entrega?*
*Los REALIZA la computadora [ ]*
*Los ARROJA la computadora <word, ws, excel, Lotus, etc.> [ ]*

*5.- ¿ Qué se hace con la información <reportes, listados > que no utiliza?*
*Destruye [ ] Tira [ ] Otro* _____

*6.- ¿ De los reportes que se le proporcionan a usted, mencione cuales no utiliza?*
_____ _____ _____ _____

*7.- De aquellos que no utiliza, por qué razón los recibe.*_____

*8.- ¿ Qué sugerencias presenta Ud. en cuanto a la eliminación de reportes, modificación, fusión ó división ?* _____

### *EVALUACIÓN DE LA INFORMACIÓN AUTOMATIZADA*

*1.- Los programas en su computadora son fáciles de utilizar?*
*SI [ ]* *NO [ ]*
*No, por qué?* _____

*2.- Con que frecuencia se presentan errores de captura de información ?*
*[ ] Diario [ ] Semanalmente [ ] Mensual [ ] Otro <especifique>*

*3.- ¿ Se hace un reporte de anomalías en la información de entrada?*
*SI [ ] NO [ ]*

*4.- ¿Maneja información confidencial a través de su computadora?*
*SI [ ] NO [ ]*

*5.- ¿Considera que es seguro el manejo de esta información?*
*SI [ ] NO [ ]*
*No, porque?* _____
_____
_____

*6.- ¿A qué módulos accesa del sistema SICOM ?*
*A todos [ ] Determinados [ ] Ninguno [ ]*

*Si tiene usted acceso a determinados módulos, mencionarlos* _____
_____

*7.- ¿Necesita clave de acceso para entrar al sistema SICOM ?*
*SI [ ] NO [ ]*

*8.- ¿El proceso de los módulos que usted maneja es de:*
*[ ] Altas [ ] Bajas [ ] Consultas [ ] Modificaciones [ ] Reportes*

## *EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*

*1.- Si en este momento perdiera la información almacenada en su computadora, su trabajo sería afectado:*
*[ ] Totalmente [ ] Parcialmente [ ] No afectaría*
*¿Por qué ?*_____
_____

*2.- ¿Quién realiza los respaldos de información almacenada en su computadora?*
*[ ] El dpto. de informática [ ] Usted [ ] No se realizan*

*3.- ¿Cómo se llevan a cabo estos respaldos?*
*[ ] Disckettes [ ] Cintas [ ] Otros <especifique>*

*4.- ¿Dónde se guardan esos respaldos?*
*[ ] En su departamento [ ] Caja de seguridad [ ] Parte externa a la empresa*
*[ ] En el dpto. de informática [ ] Otros <especifique>*

*5.- ¿Con qué frecuencia respalda la información?*
*[ ] Diario [ ] Semanalmente [ ] Catorcenalmente [ ] Mensual [ ] Otro*

*6.- ¿Cómo considera usted, en general, el servicio proporcionado por el departamento de informática en relación al manejo de la información ?*
*[ ] Deficiente [ ] Aceptable [ ] Satisfactorio [ ] Excelente [ ] Otro*

*¿Por qué?*_____

_____

## FORMATOS SUGERIDOS PARA LA RECOPILACIÓN DE LA INFORMACIÓN DE LAS DIFERENTES ÁREAS.

ÁREA DEL DEPARTAMENTO DE INFORMÁTICA

**Hoja No. ___ de ____**

**CARACTERÍSTICAS DEL PERSONAL EN LOS TRES NIVELES :**

**Autor:**_____ **Fecha:** _____

| *NIVEL* | *PERSONAL* | *USA EQUIPO* | *TIPO DE USO* | *CAPACITACION* | *ACEPTACION* |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Observaciones:**

_____

_____

_____

ÁREA DEL SOFTWARE

**Hoja No.____ de ____.**

**RELACIÓN DE SOFTWARE DE LA ORGANIZACIÓN.**
**Autor :_____ Fecha _____**

| SOFTWARE | TIPO | FUENTE | DESCRIPCIÓN | AMBIENTE | SITUACIÓN | DOCUMENTO |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

***OBSERVACIONES***

Hoja No._____ de ____ .

**RELACION DE SOFTWARE DE LA ORGANIZACION.**
**Autor :_____ Fecha _____**

| SOFTWARE | TIPO | FUENTE | DESCRIPCION | AMBIENTE | SITUACION | DOCUMENTO |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

***OBSERVACIONES***

ÁREA DEL HARDWARE

**Hoja No. ___ de**

**CONFIGURACIÓN DE EQUIPO DE CÓMPUTO PERTENECIENTE AL DEPARTAMENTO DE :**

**Autor:** _____ **fecha** _____

| CANT. | EQUIPO | CAPACIDAD | VELOCIDAD | AMBIENTE | USUARIO | ACTIVIDAD |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Observaciones:**

**RELACIÓN DE LAS FALLAS DE LOS EQUIPOS DE CÓMPUTO.**

Departamento: Pág. __ de __

| FECHA | HORA | EQUIPO | SISTEMA S | TIPO DE FALLA | TIEMPO DE REPARACION | SEGU RIDAD |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Observaciones:**

_____

_____

ÁREA DE INFORMACIÓN

**Hoja No. ___ de ____**

**RELACIÓN DEL DEPARTAMENTO DE: _____**
**CON LOS DEMÁS DEPARTAMENTOS DE LA C.E.S.P.E.**

**Autor:_____** **Fecha: _____**

| DEPARTAMENTO | DOCUMENTO | SENTIDO E / S | FRECUENCIA | MEDIO | SEGURIDAD |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Observaciones:**

*Hoja No.___ de____*

## RELACIÓN DE DOCUMENTOS QUE FLUYEN INTERNAMENTE EN LA ORGANIZACIÓN PERTENECIENTE AL DEPARTAMENTO:

***Autor:*** ***Fecha:***

| DOCUMENTO | DEPARTAMENTO ORIGEN | DEPARTAMENTO DESTINO | PRO CESO | TIEMPO RESPUESTA | | SEGU RIDAD |
|---|---|---|---|---|---|---|
| | | | | ACTUAL | REQUER. | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

***Observaciones:***

## ANEXO B

## TÉCNICAS DE PLANEACIÓN DE AUDITORÍA EN INFORMÁTICA .

1. Evaluación del personal.

Esta área debe comprender el análisis de la institución y el departamento de informática en cuestiones administrativas y políticas, se recomienda hacer esta evaluación siempre que se realice una auditoría en informática, considerando los siguientes puntos :

- Estructura.
- Normas y políticas.
- Capacitación.
- Planes de trabajo
- Controles
- Estándares.

2. Evaluación del Software.

En este apartado se deberá decidir su evaluación si encontramos situaciones en los que los sistemas puedan presentar las siguientes irregularidades :

- No estén documentados
- No existe planeación de asignación de desarrollo de sistemas
- No existe control de cartera de aplicaciones
- No existe control de cambios o actualizaciones de sistemas
- No se lleve un control de compras de software de desarrollo o aplicación.

3. Evaluación del Hardware.

Respecto a esta área se recomienda auditar, cuando se encuentren las siguientes características :

- Se tiene una variedad de configuraciones de equipos
- No están definidas políticas de adquisición de equipos.
- Equipos en aparente descuido
- Mal uso de equipo
- Inventarios irreales de equipo.

4. Evaluación de información.

Con relación a la información es importante siempre un análisis de esta área, sin embargo se recomienda con mayor razón cuando tenemos las siguientes situaciones :

- Procesos lentos dentro de la empresa
- Existencia de mucho papeleo en áreas automatizadas
- Aparente acceso sin restricción a áreas o información confidenciales.

b) Determinar tiempo y personal estimado para realizar la Auditoría en Informática.

c) Elaborar la Carta - Propuesta de Servicios Profesionales.

Una vez planeada la forma de llevar a cabo la Auditoría en Informática, estaremos en posibilidades de presentar la carta propuesta de Auditoría en Informática y el plan de trabajo **Ver Anexos C y D.**

## PROPUESTA DE SERVICIOS DE AUDITORÍA EN INFORMÁTICA

Ensenada, Baja California a 16 de Mayo de 1996.

**LIC. ALFONSO TALAVERA**
**COORDINADOR DE INFORMÁTICA**
**C.E.S.P.E.**
**C I U D A D .**

En base a nuestra conversación sostenida el día 15 de Abril del presente, en la que le solicitamos la oportunidad de realizar una Auditoria en Informática al centro de cómputo de la Comisión Estatal de Servicios Públicos de Ensenada, la cual permitirá implantar la guía que proponemos en nuestra tesis, y dar un informe o dictamen del funcionamiento del centro de cómputo, cuyo alcance será la evaluación de las siguientes áreas:

1.- Evaluación de departamento de Informática.
2.- Evaluación del Software.
3.- Evaluación del Hardware.
4.- Evaluación de la información.

Estas áreas a su vez están divididas en 4 sub áreas:

1.- Evaluación de departamento de Informática.

- Organización de área.
- Presupuestos/gastos.
- Personal de Informática.
- Personal externo.

2.- Evaluación del Software.

- Etapas de desarrollo.
- Control de proyectos.
- Monitoreo de sistemas.
- Adquisición de software general.

3.- Evaluación del Hardware.

- Adquisición de los equipos.
- Mantenimiento.
- Control de fallas.
- Uso del equipo.

4.- Evaluación de la información.

- Control de entradas/procesos/salidas.
- Acceso a la información.
- Cuidado de la información.
- Calidad de la información.

Al evaluar dichas áreas se presentará el dictamen o informe al Director General de la Organización y al Coordinador de Informática, en donde se le explicará el funcionamiento actual del centro de cómputo.

Por lo que solicitaremos información como la siguiente:

1. Para la evaluación del departamento de Informática llevaremos a cabo las siguientes actividades :

- Solicitud de los manuales administrativos, estándares utilizados y programas de trabajo.

- Elaboración de un cuestionario para la evaluación de la dirección.
- Aplicación del cuestionario al personal.
- Entrevistas a líderes de proyectos y usuarios más relevantes.
- Análisis y evaluación de la información.
- Elaboración del informe.

2. Para Evaluar el Software, contemplaremos los siguientes puntos :

- Solicitud del análisis y diseño de los sistemas en desarrollo y en operación.
- Solicitud de los manuales técnicos, del usuario, etc.
- Recopilación y análisis de los procedimientos administrativos de cada sistema.
- Flujo de información, formatos, reportes y consultas.
- Análisis de avance de proyectos en desarrollo, prioridades y personal asignado.
- Entrevista con los usuarios de los sistemas.
- Evaluación directa de la información obtenida contra las necesidades y requerimientos.
- Análisis objetivo de la estructura y flujo de los programas.
- Análisis y evaluación de la información recopilada.
- Elaboración del informe.

3).- Evaluación del Hardware.

- Solicitud de los servicios de viabilidad y características de equipos actuales.
- Solicitud de contratos de compra y mantenimiento de equipos y sistemas.
- Solicitud de contratos de seguros.
- Elaboración de cuestionarios sobre la utilización de equipos, memoria, etc.
- Visita técnica de comprobación de seguridad física y lógica de instalaciones.
- Evaluación técnica del sistema eléctrico y ambiental de los locales.
- Evaluación de la información recopilada, obtención de gráficas.

4).- Evaluación de la Información.

- Solicitud de los procedimientos de respaldo de información.
- Evaluación del contenido de los respaldos.
- Identificación del flujo de información de la empresa.
- Evaluación del control de acceso y distribución de información.

**Tiempo estimado** de la duración del proyecto de Auditoría :

1ra. etapa: Actividades de la propuesta de la Auditoría en Informática, 3 semanas.

2da. etapa: Investigación preliminar, 5 semanas.

3ra. etapa: Análisis de las áreas a auditar, 3 meses.

4ta. etapa: Reporte final, 3 semanas.

Total del tiempo : 6 meses.

Si lo anterior merece de su aprobación, solicitamos que nos lo haga saber firmando al calce, agradeciendo la oportunidad que se nos brinda, en espera de sus noticias, nos es grato saludarlo.

NOEMÍ MONTIEL HERRERA RAMONA ESTRADA SÁNCHEZ

SONIA RAQUEL SÁNCHEZ ESPINOZA

Acepto de conformidad:

Nombre: _____

Firma: _____

Cargo: _____

Fecha: _____

## ANEXO D

### CONTRATO DE AUDITORÍA EN INFORMÁTICA

Contrato de presentación de servicios profesionales de Auditoría en Informática que celebran por una parte _____, representado por _____ en su carácter de _____ y que en lo sucesivo se denominará el cliente, por otra parte _____ a quien se le denominará el auditor, de conformidad con las declaraciones y cláusulas siguientes :

**D E C L A R A C I O N E S**

**I El cliente declara :**

a) Que es una _____ ,

b) Que está representado para este acto por _____ ,
y tiene como su domicilio _____ .

c) Que requiere obtener servicios de auditoría en informática, por lo que ha decidido contratar los servicios del auditor.

**II Declara el auditor :**

a) Que es una sociedad anónima, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales está el de prestar auditoría en informática.

b) Que está constituida legalmente según escritura número ____ de fecha _____ ante el notario público núm._____ Lic. _____ .

c) Que señala como su domicilio _____
_____ .

**III Declaran ambas partes :**

a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que se contiene en las siguientes :

**C L A U S U L A S**

**PRIMERA. OBJETO**

El auditor se obliga a prestar al cliente los servicios de auditoría en informática para llevar a cabo la evaluación de la dirección de informática del cliente, que se detallan en la propuesta de servicios anexa que, firmada por las partes, forma parte integrante del contrato.

**SEGUNDA. ALCANCE DEL TRABAJO**

El alcance de los trabajos que llevará a cabo el auditor dentro de este contrato son :

a) Evaluación de la dirección de informática en lo que corresponde a :

- Estructura
- Normas y Políticas
- Planes de trabajo
- Estándares
- Recursos Humanos
- Capacitación
- Controles

b) Evaluación de los sistemas

- Evaluación de los diferentes sistemas en operación. (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).
- Opinión de los usuarios sobre los diferentes sistemas.
- Evaluación de avance de los sistemas en desarrollo y congruencia con el diseño general.
- Evaluación de prioridades y recursos asignados (humanos y equipo de cómputo)
- Seguridad física y lógica de los sistemas, su confidencialidad y respaldos.

c) Evaluación de los equipos

- Capacidades
- Nuevos proyectos
- Respaldos de equipo
- Contratos
- Utilización
- Seguridad fisica y lógica
- Seguros
- Proyecciones

d) Evaluación de información

- Solicitud de los procedimientos de respaldo de información.
- Evaluación del contenido de los respaldos.
- Identificación del flujo de información de la empresa.
- Evaluar control de acceso y distribución de información.

e) Elaboración de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos a, b, c y d de esta cláusula.

**TERCERA. PROGRAMA DE TRABAJO**

El cliente y el auditor convienen en desarrollar en forma conjunta un programa de trabajo en que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realización.

**CUARTA. SUPERVISIÓN**

El cliente o quien designe tendrá derecho a supervisar los trabajos que se le han encomendado al Auditor dentro de este contrato y a dar por escrito las instrucciones que estime convenientes.

**QUINTA. COORDINACION DE LOS TRABAJOS**

El cliente designará por parte de la organización a un coordinador del proyecto quien será el responsable de coordinar la recopilación de la información que solicite el auditor y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas.

**SEXTA. HORARIO DE TRABAJO**

El personal del auditor dedicará el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes y gozarán de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estarán sujetos a horarios y jornadas determinadas.

**SEPTIMA. PERSONAL ASIGNADO**

El auditor designará para el desarrollo de los trabajos objeto de este contrato a socios del despacho quienes, cuando consideren necesario incorporarán personal técnico capacitado de que dispone la firma, en el número que se requieran de acuerdo a los trabajos a realizar.

**OCTAVA. RELACION LABORAL**

El personal del auditor no tendrá ninguna relación laboral con el cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el auditor en ningún momento se considera intermediario del cliente respecto al personal que ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre él y su personal, y exime al cliente de cualquier responsabilidad que a este respecto existiere.

**NOVENA. PLAZO DE TRABAJO**

El auditor se obliga a terminar los trabajos señalados en la cláusula segunda de este contrato en _____ después de la fecha en que se firme el contrato y sea cobrado el anticipo correspondiente. El tiempo estimado para la terminación de los trabajos está en relación a la oportunidad en que el cliente entregue los documentos requeridos por el auditor y por el cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecidas en el programa de trabajo, sin perjuicio alguno para el auditor.

**DECIMA. HONORARIOS**

El cliente pagará al auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de _____ más el impuesto al valor agregado correspondiente. La forma de pago será la siguiente :

a) _____% a la firma del contrato

b) _____% a los _____ días hábiles después de iniciados los trabajos.

c) _____% a la terminación de los trabajos y presentación del informe final.

**DECIMOPRIMERA. ALCANCE DE LOS HONORARIOS**

El importe señalado en la cláusula décima compensará al auditor por sueldos, honorarios, organización y dirección técnica propia de los servicios de auditoría, prestaciones sociales y laborales de su personal.

**DECIMOSEGUNDA. INCREMENTO DE HONORARIOS**

En caso de que se tenga un retraso debido a la falta de entrega de información, demora o cancelación de las reuniones, o cualquier otra causa imputable al cliente, este contrato se incrementará en forma proporcional al retraso y se señalará al incremento de común acuerdo.

**DECIMOTERCERA. TRABAJOS ADICIONALES**

De ser necesaria alguna adición a los alcances o productos del presente contrato, las partes celebrarán por separado un convenio que formará parte integrante de este instrumento y en forma conjuntan se acordará el nuevo costo.

**DECIMOCUARTA. VIATICOS Y PASAJES**

El importe de los viáticos y pasajes en que incurra el auditor en el traslado, hospedaje y alimentación que requieran durante su permanencia en la ciudad de _____: Como consecuencia de los trabajos objeto de este contrato, será por cuenta del cliente.

**DECIMOQUINTA. GASTOS GENERALES**

Los gastos de fotocopiado y dibujo que se produzcan con motivo de este contrato correrán por cuenta del cliente.

**DECIMOSEXTA. CAUSAS DE RESCISION**

Serán causas de rescisión del presente contrato la violación o incumplimiento de cualquiera de las cláusulas de este contrato.

**DECIMOSEPTIMA . JURISDICCION**

Todo lo no previsto en este contrato se regirá por las disposiciones relativas, contenidas en el código civil de _____, en su caso de controversia para su interpretación y cumplimiento, las partes se someten a la jurisdicción de los tribunales federales, renunciando al fuero que les pueda corresponder en razón de su domicilio presente o futuro.

Enteradas las partes del contenido y alcance legal de este contrato, lo firman de conformidad en original y tres copias, en la ciudad de _____ , el día _____ .

# *CÓDIGO DE ÉTICA PROFESIONAL*

Los Auditores de sistemas de Información deberán:

- **APOYAR** el establecimiento y cumplimiento con adecuados estándares.
- **CUMPLIR** con los estándares de Auditoría de sistemas de Información tal como han sido adoptados por la Electronic Data Proscessing Auditors Foundation.
- **SERVIR** a los intereses de sus empleados, accionistas, clientes y al público en general de una manera diligente, leal y honesta; no deberá participar con conocimiento de ninguna actividad ilegal o impropia.
- **MANTENER** la confidencialidad de la Información obtenida en el curso de sus deberes.
- **DESEMPEÑAR** sus deberes de una manera objetiva e independiente, y deberá evitar actividades que pongan en riesgo o que aparenten poner en riesgo su independencia.
- **MANTENER** su competencia en los campos interrelacionados de la Auditoría y de los sistemas de Información a través de participar en actividades de desarrollo profesional.
- **PONER** el debido cuidado en obtener y documentar los suficientes hechos materiales en los cuales base sus conclusiones y recomendaciones.
- **INFORMAR** a las partes apropiadas los resultados de la Auditoría realizada.
- **APOYAR** la educación de la Administración, clientes y público en general a mejorar su comprensión de la Auditoría de sistemas de Información.
- **MANTENER** altos estándares de carácter y conducta tanto en actividades profesionales como personales.

# NORMAS, REGLAMENTOS Y BASES LEGALES DE LA AUDITORÍA EN INFORMÁTICA.

**Normas y lineamientos que regulan el funcionamiento de los órganos internos de control .**

El presente documento (tomado del diario oficial), tiene el propósito de establecer los lineamientos de carácter general que normen la ejecución de la Auditoria de los sistemas automatizados.

**LINEAMIENTOS :**

I. PLANEACIÓN.

1.- Comprobar que exista un comité de Informática, integrado por personal clave de todas las áreas usuarias y que sea el que establezca prioridades para la función.

2.- Verificar que la función se encuentre debidamente planeada a corto, mediano y largo plazo, de acuerdo a lo siguiente :

- Planes sectoriales, programas prioritarios y criterios de austeridad.
- Estudio de costos y beneficios derivados de la introducción de equipo de cómputo para el procesamiento de la información.
- Un plan maestro de los objetivos a largo plazo de la instalación de cómputo, así como de las tareas necesarias para darles cumplimiento.
- Planes para la adquisición o cambios de recursos de cómputo (Hardware y software), si es que esto se requiere.
- Un proyecto de desarrollo de los sistemas que asegure que estos son consistentes con las metas y objetivos establecidos en el plan maestro.
- Un plan de recuperación de archivos y programas para el caso de alguna eventualidad.

3.- Revisar si los presupuestos de inversión se encuentran debidamente aprobados por las instancias correspondientes, que se ejerzan conforme a calendario y que las variaciones sean analizadas, aclaradas y justificadas, así como que existan las modificaciones correspondientes.

II. ORGANIZACIÓN.

1.- Verificar que la estructura orgánica del área de administración y control de sistemas automatizados esté debidamente autorizada, sea vigente atienda a criterios de racionalidad y cuente con el nivel jerárquico apropiado que le permita desarrollar adecuadamente las funciones correspondientes.

2.- Comprobar la existencia y vigencia de adecuadas descripciones de funciones y perfiles requeridos para cada puesto.

3.- Cerciorarse de que existan programas de adiestramiento y capacitación que permitan contar con personal calificado para el adecuado desarrollo de la función.

4.- Verificar que exista un análisis sistemático de cargas de trabajo que permita determinar la insuficiencia o exceso de recursos humanos y comprobar, en su caso, el cumplimiento oportuno de los programas de ajuste de personal.

5.- Revisar que se cuente con los recursos técnicos y materiales necesarios para llevar a cabo la función.

6.- Comprobar que se haya adaptado una adecuada división de actividades y asignación de responsabilidades de acuerdo con las funciones, tanto en la propia área como en los departamentos de origen y los usuarios.

7.- Comprobar que existan objetivos particulares, claros, precisos y congruentes con los generales de la Dependencia o Entidad.

8.- Revisar que existan manuales de Organización, políticas y procedimientos, que se encuentren actualizados, sean del conocimiento del personal y se apliquen.

9.- Cuando la Dependencia o Entidad cuente con unidades en el interior del país, verificar que exista una adecuada desconcentración de la función de administración, y control de los sistemas automatizados, a fin de procurar que los trámites se lleven a cabo y resuelvan en los mismos lugares donde se originen las operaciones, a traves de una adecuada delegación de funciones y mecanismos de supervisión que aseguren su apropiado cumplimiento.

10.- Comprobar la existencia de programas tendientes a la simplificación administrativa que promuevan la agilización, transparencia y reducción de trámites.

III. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

1.- Verificar que el diseño y desarrollo de los sistemas se lleve a cabo conforme a los objetivos establecidos en la planeación de largo plazo.

2.- Determinar si los recursos humanos y de cómputo disponibles permiten llevar a cabo los planes de desarrollo de sistemas.

3.- Verificar que previamente al inicio del diseño de sistemas, se llevaron a cabo y se encuentren debidamente documentadas las siguientes actividades:

- Definición clara del problema a resolver con el procesamiento electrónico de datos (PED).
- Descripción de los objetivos del nuevo sistema, así como de las limitaciones de recursos y de organización.
- Aprobación formal para iniciar el proyecto.
- Estudio preliminar del sistema para evaluar la factibilidad de automatizarlo y que comprenda la determinación de los recursos técnicos requeridos para soportarlo, las posibilidades de obtener los datos a procesar, la utilización de los productos que se esperan, la identificación del impacto que tendrá el sistema en la Organización y en los procedimientos de los usuarios, así como la determinación de costos y beneficios que se obtendrán.

4.- Verificar que en el diseño de sistemas se consideren:

- Volúmenes de información a procesar.
- Áreas de almacenamiento de información requeridas.
- Tiempos de respuesta requeridos.
- Facilidades de programación.
- Limitaciones de la integridad de los datos.
- Uso que se dará a la información procesada (toma de decisiones, control administrativo, etc.).

5.- Evaluar el diseño de sistemas en los siguientes aspectos; flujo de información, archivos o bases de datos, especificaciones de los programas de computadora y especificaciones de los recursos de cómputo a utilizar.

6.- Verificar que el diseño de procedimientos y formas, así como los manuales de los usuarios sean claros, precisos y estén de acuerdo con el diseño técnico de los sistemas.

7.- Comprobar que se lleven a cabo pruebas finales del sistema y que para ello se contempló lo siguiente:

A) Planeación de las pruebas.

B) Diseño y desarrollo de los datos de prueba.

C) Evaluación de los resultados.

D) Adopción de medidas para corregir el sistema, en caso de existir errores.

8.- Verificar que se lleven a cabo correctamente, las siguientes actividades, previamente a la puesta en operación del nuevo sistema:

- Capacitación del personal usuario.
- Capacitación del personal de PED en caso de que se hubieran cambiado o introducido nuevos recursos de cómputo.
- Conversión de archivos y programas al formato necesario para el nuevo sistema.
- Calendarización de las operaciones y corridas de prueba.

9.- Evaluar la corrección del proceso de conversión de los archivos maestros.

10.- Verificar que en el desarrollo de sistemas participen las áreas usuarias en cada una de las siguientes fases:

- Previamente al inicio de sistemas, para revisar y autorizar
- Durante el desarrollo, para revisar el avance y compararlo con lo previsto.
- En las pruebas finales, para aprobar.

11.- Verificar que se cuente con estándares para elaborar los programas de cómputo y evaluar que sean correctos de acuerdo con los recursos disponibles.

12.- Comprobar que los programas de cómputo se formulen de acuerdo con los estándares establecidos.

13.- Verificar que se mantenga un control de las modificaciones a los sistemas y programas y sea establecido algún mecanismo para que los usuarios estén conscientes de los costos de cada modificación.

15.- Comprobar que previamente al inicio de alguna modificación se obtiene la autorización ya sea de los niveles directivos cuando sean cambios importantes o de los empleados principales de los departamentos usuarios cuando se trate de modificaciones menores.

16.- Verificar que se efectúen pruebas de las modificaciones, que las mismas son aprobadas por los departamentos usuarios y que se actualice la documentación del sistema como resultado de los cambios.

17.- Verificar que los operadores no efectúen modificación alguna a los sistemas y programas.

18.- Verificar que el área de operaciones sólo acepte las modificaciones que están debidamente aprobadas.

IV OPERACIÓN DE LA COMPUTADORA

1.- Verificar que exista y se ponga en práctica el manual de métodos y procedimientos de ejecución para los operadores de la computadora, en lo referente a las actividades:

- Encendido y apagado del equipo
- Acciones a adoptar en caso de fallas del sistema
- Tiempos estándar para montar y desmontar los dispositivos de almacenamiento
- Descripción de las actividades prohibidas.

2.- Verificar que existan y se pongan en práctica las instrucciones para correr cada uno de los sistemas en producción y que se haya establecido el estándar de consumo de recursos cuando los sistemas operan normalmente.

3.- Comprobar que se han establecido los procedimientos tradicionales de control interno: rotación de personal, entrenamiento adecuado, programación adecuada de vacaciones, asignación de dos o más operadores para la operación de los sistemas, críticos, prohibición a los operadores para conocer a detalle la lógica de los sistemas.

4.- Verificar que se examinen periódicamente las actividades de los operadores a través de los registros del sistema operativo (cuando exista esta facilidad), que se supervisen e investiguen las desviaciones importantes con respecto a los estándares establecidos.

5.- Verificar que existan y evaluar que sean correctos, los controles de uso del equipo de cómputo para: correr sistemas en producción, procesos, actividades de desarrollo de sistemas, etc.

6.- Verificar que se revisen periódicamente los reportes de los operadores sobre el mantenimiento preventivo y correctivo que se da al equipo, que se investiguen desviaciones y se adopten las medidas necesarias.

7.- Verificar que el personal que controla la recepción-entrega de datos a los usuarios, no tenga funciones de captura y procesamiento.

8.- Evaluar que los métodos y procedimientos implantados en la sección de control, sean adecuados de acuerdo con las características de la información que entra y sale del área de PED y con la magnitud de la instalación.

9.- Verificar que la sección de biblioteca cuenta con instructivos para:

- Ordenar y mantener adecuadamente los archivos.
- Mantener un registro de cada uno de los archivos para identificarlos por: nombre, programas y personal responsable del archivo, versión, requerimientos de respaldo, etc.

10.- Revisar y evaluar que los controles establecidos para la documentación de los sistemas, programas y manuales de los operadores y de los usuarios, permitan:

- Conservarla en forma segura
- Ponerla a disposición solamente del personal autorizado.
- Mantener un respaldo adecuado.

11.- Verificar que se cuente con planes de recuperación en casos de desastre y revisar que contengan como mínimo:

- Enumeración de los posibles riesgos para la instalación de cómputo y una evaluación de la importancia de tales riesgos.
- Las medidas preventivas y correctivas a considerar y los costos que le son inherentes.
- Recomendaciones de las medidas preventivas que deben implantarse.

12.- Verificar que se hayan implantado las medidas de seguridad aprobadas.

13.- Comprobar que sólo el personal autorizado tiene acceso al área donde se ubica el equipo de cómputo.

## V. CONTROLES DE LAS APLICACIONES AUTOMATIZADAS

1.- Evaluar los métodos y controles aplicables a la captura, así como a la preparación e ingreso de datos a la computadora, que permitan la operación de la aplicación en forma eficiente y eficaz, la salvaguarda de activos y la integridad de la información.

2.- Evaluar si el diseño de los documentos fuente que se utilizan en la aplicación, permiten registrar los datos en forma rápida y precisa, controlar el flujo de trabajo, facilitar la conversión de los datos a forma legible para la máquina y facilitar la verificación de los datos capturados.

3.- Comprobar que existan y evaluar que sean adecuados, los controles de captura de ingreso de datos, tales como; dígitos de verificación y totales de control.

4.- Verificar que se cuente con manuales actualizados de los procedimientos para recibir, capturar y regresar los documentos fuente.

5.- Determinar si los mecanismo para controlar el acceso a la computadora tienen la capacidad para controlar tanto la entrada como el uso de los recursos, a través de: identificación de los usuarios autorizados, de los recursos que pueden utilizar y los privilegios que tienen con respecto a los recursos.

6.- Comprobar que existan y sean adecuados, los controles establecidos en los programas de cómputo que permiten la entrada de datos, para :

- Validarlos automáticamente.
- Manejar y reportar errores.

7.- Revisar y comprobar que los programas de cómputo diseñados para la aplicación permiten:

- Validar los resultados del procesamiento de la información (por ejemplo: rangos permitidos para determinados datos, signos totales de control etc.).
- Asegurar que se procesan todos los registros y los archivos.
- Procesar los cambios de los archivos maestros, antes de su actualización.
- Manejar correctamente el redondeo de cifras.
- Imprimir cifras de control en cada paso del procesamiento.
- Imprimirla información de las tablas que manejan los programas de cómputo.
- Minimizar la intervención de los operadores.

8.- Verificar que los controles sobre los reportes que emite la aplicación sean adecuados, de acuerdo con el grado de confiabilidad de la información que contienen y con la forma en que se producen (en lote o interactivamente).

9.- Verificar que los controles sobre archivos magnéticos que se generan, sean adecuados para la aplicación de que se trate( por ejemplo, el uso de etiquetas internas, número de versión del archivo, plazo de retención, totales de control, etc.).

10.- Dada la magnitud y naturaleza de la aplicación, así como la importancia de los datos que maneja, verificar que se cuente con archivos que permitan rastrear las transacciones desde su origen, a través de algún o algunos datos, hasta su situación actual y viceversa, esto es, reconstruir las transacciones a través de algún o algunos datos.

11.- Evaluar si se cuenta con el software adecuado para que tales archivos permitan:

- Conocer la situación de los datos importantes durante un período.
- Evaluar el funcionamiento del sistema a través del rastreo de transacciones.
- Identificar las consecuencias de algún error mediante el registro de quienes tuvieron acceso a la información.

12.- Dada la magnitud de la instalación de cómputo y de los sistemas que se manejan, verificar que existan archivos con la información de los eventos que ocurren al correr la aplicación, tales como; consumo de recursos, intentos fallidos de utilizar los recursos, fallas de hardware, etc.

VI. PRODUCTIVIDAD DE LA FUNCIÓN

1.- Verificar que se realicen estudios tendientes a apoyar los cambios que se operan en los sistemas de control de las áreas usuarias y a establecer programas para el mejor aprovechamiento de los recursos materiales, tecnológicos y humanos.

2.- Comprobar que existan mecanismo o instrumentos de autoevaluación tendientes a lograr la economía, eficiencia, eficacia y efectividad del control y administración de los recursos y que las medidas preventivas y/o correctivas que de ellos se deriven, se pongan en práctica.

3.- Verificar la productividad de la función mediante la revisión de metas, objetivos, indicadores y la comparación de éstos con el apoyo que efectivamente proporciona a las áreas usuarias.

# ESTÁNDARES GENERALES PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN .

**Independencia.**

Estándar general No.1 **Actitud y Apariencia:**

En cualquier materia relacionada con la Auditoría, el Auditor de sistemas de información debe ser independiente en actitud y apariencia.

Estándar General No.2 **Relación Organizacional:**

La función de Auditoría de sistemas debe ser suficientemente independiente del área a ser Auditada para permitir una realización objetiva de la Auditoría.

Estándar General No.3 **Código de Ética Profesional:**

El Auditor de sistemas de información debe adherirse al Código de Ética Profesional de la Electronic Data Proscessing (EDP) Auditors Foundation.

**Competencia Técnica.**

Estándar General No.4 **Habilidades y Conocimientos:**

El Auditor de sistemas de información debe ser técnicamente competente, y poseer las habilidades y conocimientos necesarios para realizar el trabajo de Auditoría.

Estándar General No.5 **Educación Profesional Continua:**

El Auditor de sistemas de información debe mantener su competencia técnica a través de su propia educación continua.

**Desarrollo de trabajo .**

Estándar General No. 6 **Planeación y Supervisión:**

Las Auditorías de sistemas de información deben ser planeadas y supervisadas para proporcionar el aseguramiento de que los objetivos de Auditoría se alcancen y que se de cumplimiento a los estándares.

Estándar General No.7 **Requerimiento de evidencias:**

Durante el curso de la Auditoría, el Auditor de sistemas de información deberá obtener evidencias en naturaleza y suficiencia para soportar los hallazgos y conclusiones reportadas.

Estándar General No. 8 **Cuidado Profesional :**

Debe ejercerse cuidado profesional en los aspectos del trabajo de Auditoria, incluyendo la observancia y aplicación de los estándares de Auditoria .

Reportar General No. 9 **Reportar la Curva de la Auditoría:**.

Al preparar los reportes, el Auditor de sistemas de información debe establecer los objetivos de Auditoría, el periodo de cobertura y la naturaleza y extensión del trabajo de Auditoría desarrollado.

Estándar General No. 10 **Reportar los hallazgos y las conclusiones:**

Al preparar los reportes el Auditor de sistemas de información debe establecer los hallazgos y conclusiones concernientes al trabajo de Auditoría desarrollado y cualquier reserva o calificación que el Auditor tenga con respecto a la Auditoria.