



**UNIVERSIDAD MICHOACANA DE
SAN NICOLAS DE HIDALGO**



**FACULTAD DE CONTADURIA Y
CIENCIAS ADMINISTRATIVAS**

TESINA

**AUDITORIA INFORMATICA EN LA
JURISDICCION SANITARIA PATZCUARO**

QUE PARA OBTENER EL TITULO DE

LICENCIATURA DE INFORMATICA ADMINISTRATIVA

ASESOR

M. A. HILDA RODALES TRUJILLO

PRESENTA

RODRIGO AGUIRRE RANGEL

Morelia, Mich., julio de 2011

Índice

INTRODUCCION.....	1
PROBLEMÁTICA.....	3
OBJETIVOS.....	4
JUSTIFICACION.....	5
CAPITULO 1: AUDITORIA INFORMATICA	
1.1 IMPORTANCIA DE LA AUDITORIA INFORMÁTICA	7
1.2 FORMAS DE REALIZAR UNA AUDITORIA INFORMÁTICA	8
1.3 SÍNTOMAS DE NECESIDAD DE AUDITORIA INFORMÁTICA	9
1.4 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA	9
1.5 PROCEDIMIENTO PARA LA AUDITORÍA INFORMÁTICA	10
1.5.1 Planeación de la Auditoria Informática	10
1.5.2 Identificación de Necesidades	11
1.5.3 Investigación Preliminar	11
CAPITULO 2: AUDITORIA DE LA FUNCION INFORMATICA	
2.1 RECOPIACIÓN DE LA INFORMACIÓN ORGANIZACIONAL.....	13
2.1.1 Estructura Organizacional.....	13
2.1.2 Situación de los Recursos Humanos.....	13
2.1.3 Entrevistas con el Personal de Informática.....	13
2.1.4 Situación Presupuestal y Financiera.....	13
2.2 PRINCIPALES DOCUMENTOS QUE SE NECESITAN.....	14
2.2.1 Estudio de Viabilidad	14
2.2.2 Plan de Cambios, Modificaciones y Actualización.....	14
2.2.3 Planes Estratégicos o Maestro	14
2.2.4 Plan de Proyectos.....	14
2.2.5 Plan de Seguridad	15
2.3 FUNCIONES Y OBJETIVOS	15
CAPITULO 3: AUDITORIA DE LOS SISTEMAS	
3.1 EVALUACIÓN DE LOS SISTEMAS	17
3.2 EVALUACIÓN DEL ANÁLISIS.....	17
3.3 EVALUACIÓN DEL DISEÑO LÓGICO DEL SISTEMA	19
3.4 PROGRAMAS DE DESARROLLO	19
3.4.1 Bases de Datos.....	20
3.5 COMUNICACIÓN.....	21
3.5.1 Ruido, Redundancia y Entropía.....	21
3.6 EVALUACIÓN DEL DESARROLLO DE SISTEMA.....	22
3.7 SISTEMAS DISTRIBUIDOS, INTERNET, COMUNICACIÓN ENTRE OFICINAS	22
3.7.1 Control de Proyectos.....	22
3.8 CONTROL DE DISEÑO DE SISTEMAS Y PROGRAMACIÓN	22
3.9 INSTRUCTIVOS DE OPERACIÓN.....	23
3.10 FORMA DE IMPLANTACIÓN	23
3.11 EQUIPO Y FACILIDADES DE PROGRAMACIÓN.....	24
3.12 ENTREVISTAS A USUARIOS.....	24
CAPITULO 4: EVALUACION DEL PROCESO DE DATOS Y EQUIPO DE CÓMPUTO	
4.1 CONTROLES	26
4.1.1 Políticas de Respaldo	26
4.1.2 Políticas y Procedimientos	27

4.1.3 Políticas de Bitácoras.....	27
4.1.4 Control de las Licencias de Software	27
4.2 CONTROL DE DATOS FUENTE Y MANEJO DE CIFRAS DE CONTROL.....	27
4.3 CONTROL DE OPERACIÓN.....	28
4.4 CONTROL DE ASIGNACIÓN DE TRABAJO	28
4.5 CONTROL DE MEDIOS DE ALMACENAMIENTO MASIVO	28
4.6 CONTROL DE MANTENIMIENTO	28
4.7 ORDEN EN EL CENTRO DE CÓMPUTO	29
4.8 CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO.....	29
4.9 PRODUCTIVIDAD.....	29
4.10 EQUIPOS DE CÓMPUTO	29

CAPITULO 5: EVALUACION DE LA SEGURIDAD

5.1 SEGURIDAD LÓGICA Y CONFIDENCIALIDAD	31
5.2 SEGURIDAD LÓGICA.....	31
5.2.1 Rutas de Acceso.....	32
5.2.2 Claves de Acceso	32
5.2.3 Software de Control de Acceso.....	33
5.2.4 Encriptamiento	34
5.3 SEGURIDAD EN EL PERSONAL	34
5.4 SEGURIDAD FÍSICA.....	34
5.5 UBICACIÓN Y CONSTRUCCIÓN DEL CENTRO DE CÓMPUTO.....	35
5.6 PISO ELEVADO O CÁMARA PLENA	35
5.7 AIRE ACONDICIONADO.....	35
5.8 INSTALACIÓN ELÉCTRICA Y SUMINISTRO DE ENERGÍA	35
5.8.1 Reguladores.....	36
5.9 SEGURIDAD CONTRA DESASTRES PROVOCADOS POR AGUA.....	36
5.10 SEGURIDAD DE AUTORIZACIÓN DE ACCESOS	36
5.11 DETECCIÓN DE HUMO Y FUEGO, EXTINTORES	36
5.12 TEMPERATURA Y HUMEDAD	37
5.13 SEGURIDAD EN CONTRA DE VIRUS	37

CAPITULO 6: APLICACIÓN DEL CASO

6.1 MARCO DE REFERENCIA.....	39
6.1.1 Descripción estratégica de la organización (Giro, Misión, Visión, Organigrama).....	39
6.1.2 Antecedentes.....	40
6.2 AUDITORIA DE LA FUNCIÓN INFORMÁTICA	41
6.2.1 Alcance y Objetivos del área	41
6.2.2 Cuestionario	41
6.2.3 Hallazgos Encontrados.....	42
6.2.4 Conclusiones.....	43
6.2.5 Recomendaciones	43
6.3 EVALUACIÓN DE LOS SISTEMAS	45
6.3.1 Alcance y Objetivos	45
6.3.2 Cuestionario	45
6.3.3 Hallazgos Encontrados.....	46
6.3.4 Conclusiones.....	47
6.3.5 Recomendaciones	47
6.4 EVALUACIÓN DEL PROCESAMIENTO DE DATOS Y EQUIPOS DE CÓMPUTO	48
6.4.1 Alcance y Objetivos	48
6.4.2 Cuestionario	48
6.4.3 Hallazgos Encontrados.....	49
6.4.4 Conclusiones.....	50
6.4.5 Recomendaciones	51
6.5 EVALUACIÓN DE SEGURIDAD.....	52

U.M.S.N.H.

F.C.C.A.

Auditoría Informática en la Jurisdicción Sanitaria Pátzcuaro

6.5.1 Alcance y Objetivos	52
6.5.2 Cuestionario	52
6.5.3 Hallazgos Encontrados.....	53
6.5.4 Conclusiones.....	54
6.5.5 Recomendaciones	54
7. DICTAMEN FINAL	55
8. CONCLUSIONES	63
BIBLIOGRAFIA	63

INTRODUCCIÓN

La Administración se define como el proceso de crear, diseñar y mantener un ambiente en el cual las personas al laborar o trabajar en grupos, alcancen con eficiencia metas seleccionadas. Las personas realizan funciones administrativas de planeación, organización, integración de personal, dirección y control.

- La administración se aplica en todo tipo de organización.
- Es aplicable en todos los niveles de las organizaciones.
- La administración se ocupa del rendimiento; esto implica eficacia y eficiencia.

Auditoría es un examen crítico y sistemático que se realiza a una persona o grupo de personas, a procesos, métodos o mecanismos, sistemas y áreas o departamentos, con el fin de detectar errores y señala fallas.

Informática es la ciencia que se encarga del estudio y aplicación sistemática de las tecnologías de información y comunicación, métodos, herramientas y técnicas relacionadas con las computadoras y el procesamiento de la información por medios electrónicos, orientada al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya de manera oportuna y eficaz.

Función o Dirección Informática, es una serie de procedimientos que ayudan a organizar, controlar y coordinar el funcionamiento técnico y administrativo en un centro de cómputo.

En la actualidad organizacional las Tecnologías de Información ya no puede considerarse sólo como un simple apoyo, por el contrario, su rol ha llegado a ser el de una función esencial. Así las cosas, el despilfarro computacional puede entenderse como un fenómeno organizacional caracterizado por el uso inapropiado de las Tecnologías de Información, que no solo implica graves perjuicios económicos, sino que afecta el ejercicio

de la empresa. Tal fenómeno se debe principalmente a la carencia de una adecuada administración de Tecnologías de Información.

Diversas situaciones hacen explícito el despilfarro computacional. No obstante, quienes tienen contacto directo con la realidad informática de las empresas, estarán de acuerdo en que tales situaciones resultan igualmente comprobables, al punto de generalizarse la creencia absurda de que se encuentran implícitas en la forma de trabajo del profesional informático.

El procesamiento electrónico de datos comenzó en la década de 1950 para llevar las cuentas y el registro de actividades en las organizaciones. Al poco tiempo inició el interés por auditar los sistemas de información, los procesos de negocios apoyados por estos, los datos financiero-contables, la infraestructura tecnológica y la seguridad informática.

Se someten a examen las actividades apoyadas por las Tecnologías de Información para revisar los controles, el cumplimiento con políticas y regulaciones, así como el grado en el cual estas apoyan la eficiencia, eficacia y rentabilidad económica.

Estas auditorías ayudan a las organizaciones a evaluar la manera en que proveen sus servicios apoyados por Tecnologías de Información, buscando proteger los intereses de socios, empleados y clientes. Esto permite validar la seguridad, confiabilidad, integridad y privacidad de los sistemas de información.

Los auditores informáticos pueden recomendar cambios en los procesos de servicios para lograr los objetivos sociales de la organización. También es posible que las investigaciones revelen fraudes, desperdicios o abusos. Los auditores informáticos modernos proceden de manera sistemática en sus estudios, planificando sus acciones y enfocándose en las áreas de mayor riesgo.

Dada la dependencia creciente de las organizaciones en las Tecnologías Información y el surgimiento de normativa para su buen gobierno, el auditor informático también trabaja como consejero, asesorando en cuanto al establecimiento de políticas y estándares que aseguren la información y el control de las Tecnologías de Información.

PROBLEMÁTICA

La estructura operativa como área de informática es inadecuada en la jurisdicción ya que cuenta un elevado número de personal, así como aumento de las tecnologías de información y comunicación. La falta de planes, programas y procedimientos de trabajo impiden un mejor funcionamiento de las funciones del área de informática.

Inexistentes controles de administración de las tecnologías de información, debido a desconocimiento e implementación de un procedimiento por las autoridades locales y estatales.

Delimitar funciones del área de informática, ya que en algunos departamentos se toman decisiones con respecto a los sistemas y equipos de cómputo sin consultar el área informática.

Falta de programas de evaluación y control del personal ya que no se cuenta con capacitación continua, y el personal informático se encuentra en un rezago o desventaja competitiva con otras organizaciones.

Despilfarro Informático originado por el desconocimiento y mal uso de las tecnologías de información. Mala aplicación de recurso financiero, porque este es en ocasiones desviado para comprobar otras necesidades, ya que está controlado por el administrador y el coordinador del programa en salud.

Inadecuados procesos de estudio, evaluación y beneficios en la adquisición de T.I., se adquieren equipos ensamblados para cubrir necesidades urgentes, sin considerar el tiempo de vida útil de estos equipos de cómputo.

OBJETIVO PRINCIPAL

Revisión a la administración de la función informática en la Jurisdicción Sanitaria Pátzcuaro, siguiendo la metodología establecida por José Antonio Echenique García.

OBJETIVOS PARTICULARES

- Revisar y evaluar la Función Informática.
- Revisar y evaluar los Sistemas en desarrollo y operación.
- Revisar y evaluar el Procesamiento de Datos y los Equipos de Cómputo.
- Revisar y evaluar la Seguridad.

JUSTIFICACIÓN

Actualmente en las diferentes áreas se cuenta con tecnologías de información rebasadas en características de acuerdo con los requerimientos necesarios para el funcionamiento de los sistemas de información.

No se lleva a cabo una actualización programada de las tecnologías de información, lo que repercute en el adecuado funcionamiento de las áreas responsables.

Adquisiciones mal realizadas por el área financiera ya que no contempla o solicita un diagnóstico situacional de necesidades de tecnologías de información para las áreas involucradas.

Falta de aplicación de evaluaciones al personal usuario de las tecnologías de información sobre el uso y mantenimiento. No existe un inventario de licencias originales de los sistemas de información así como la documentación de las pólizas de garantía.

No se ha contemplado auditoría informática de forma interna y tampoco externa para identificar despilfarro informático de cada una de las áreas involucradas con tecnologías de información.

Por lo anterior se crea la necesidad de administrar y controlar las tecnologías de información con procesos que ayuden al área de informática a tomar o sugerir decisiones a los directivos sobre las necesidades de invertir en tecnologías de información.

Sugerir mecanismos de control eficientes para el uso de las tecnologías de información.

CAPITULO 1: AUDITORIA INFORMATICA

La auditoría informática es la revisión y evaluación de los controles, sistemas de información y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio de señalamientos logre una utilización más eficiente, confiable y segura de la información, que servirá para la toma de decisiones.

1.1 Importancia de la Auditoria Informática

Las Tecnologías de Información, consideradas como el hardware, software, sistemas de información, redes locales, bases de datos, telecomunicaciones, desarrollo de software, servicios y organización de informática, es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a las organizaciones frente a sus similares en el mercado, pero puede generar costos y desventajas si no es bien administrada por el personal informático.

Para darse cuenta si se está administrando de manera correcta la función informática es necesario que se evalúe con dicha función mediante evaluaciones oportunas y completas por personal calificado consultores externos, auditores en informática evaluaciones periódicas realizadas por el mismo personal informático.

Las auditorías son necesarias por diversos motivos, y entre los más importantes podemos citar los siguientes:

- Ofrecer la seguridad a las partes interesadas en las organizaciones auditadas o a los responsables de sus actividades, de la fiabilidad de los estados financieros que se les presentan, en la medida indicada por el auditor en su informe.
- Ofrecer la seguridad a otros posibles usuarios de la información, de la fiabilidad de los datos que se les presentan, en la medida indicada por el auditor en su informe.

- Estos usuarios pueden ser: directivos, autoridades estatales, personal, Hacienda Pública, población usuaria e instituciones y organizaciones no gubernamentales.
- Cuando se realiza un cambio de titularidad o cambio de secretario, es necesario conocer la fiabilidad de dicha organización.

1.2 Formas de realizar una Auditoria Informática

La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la organización auditada. Los empleados que realizan esta actividad son remunerados económicamente. Esta auditoría existe por decisión de la organización y esta puede optar por su disolución en cualquier momento.

Este tipo de auditoría cuenta con algunas ventajas adicionales muy importantes respecto a la auditoría externa, las cuales no son tan perceptibles como en las auditorías convencionales:

- Actuación periódica realizando revisiones globales, como parte de su plan de trabajo anual y de su actividad normal.
- Los auditores conocen estos planes y se habitúan a las auditorías.
- En la organización los responsables de informática escuchan, orientan e informan sobre las posibilidades de técnicas y costos de tal sistema.

La organización necesita controlar su informática y está; necesita que su propia gestión sometida a los mismos procedimientos y estándares que el resto de aquella. En cuanto a la organización se refiere solamente las más grandes pueden aplicar una auditoría propia y permanente, mientras que el resto acuden a auditores externos. Finalmente, la propia informática necesita de su propio grupo de control interno, con implantación física en su estructura, puesto que si se ubicase dentro de la estructura informática ya no sería independiente.

Por otro lado, la auditoría externa es realizada por personas ajenas a la organización auditada y siempre genera un costo. Se presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados.

1.3 Síntomas de necesidad de Auditoría Informática

Las organizaciones acuden a las auditorías en informática cuando existen síntomas perceptibles de debilidad. Estos síntomas pueden clasificarse de la siguiente manera:

- Síntomas de descoordinación y desorganización,
- Síntomas de mala imagen e insatisfacción de los usuarios,
- Síntomas de debilidades económico-financieras,
- Síntomas de inseguridad.

1.4 Herramientas y Técnicas para la Auditoría Informática

Cuestionarios

La auditoría informática se materializa en la recopilación de información y documentación de todo tipo. Para esto suele ser habitual comenzar solicitando la complementación de cuestionarios impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación y muy cuidados en su fondo y forma.

Sobre esta base, se estudia y analiza la documentación recibida de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Esta fase puede omitirse cuando se haya adquirido por otros medios la información que aquellos cuestionarios hubieran proporcionado.

Entrevistas

El auditor realiza una conversación con el auditado dirigida con el objetivo de recabar información mediante un formato de preguntas y respuestas. La entrevista será dirigida a la persona indicada y responsable del área a evaluar.

La entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio. El auditor informático entrevista al auditado siguiendo un sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud una serie de preguntas variadas. Tras la entrevista debe existir una preparación muy elaborada y sistemática y que es diferente para cada caso particular.

1.5 Procedimiento para la Auditoría Informática

1.5.1 Planeación de la Auditoría en informática

Para llevar a cabo una adecuada planeación hay que seguir una serie de pasos previos que permitirán identificar el tamaño y las características del área dentro de la organización a auditar, sus sistemas, organización y equipo, para determinar el número y las características del personal de auditoría, las herramientas necesarias, el tiempo y el costo, así como definir los alcances de la auditoría.

Es necesario hacer una investigación preliminar y algunas entrevistas previas, y con base a esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular el desarrollo de las mismas.

1.5.2 Identificación de necesidades

- ✓ Desorganización del área de Informática
- ✓ Desconcentración del área de informática
- ✓ Falta de un presupuesto
- ✓ Mala distribución de los Equipos de cómputo e impresoras
- ✓ Falta de programas de mantenimiento
- ✓ Descontrol en consumibles (Papel, Tóner, CD, etc.)
- ✓ No se cuenta con Software Antiviral, Ofimática, etc., originales
- ✓ Instalaciones inadecuadas
- ✓ Aumento de tecnologías de información
- ✓ Despilfarro informático

1.5.3 Investigación preliminar

Se debe recopilar información para obtener una visión general del departamento a través de observaciones, entrevistas preliminares y solicitudes de documentos con la finalidad de definir el objetivo y alcance de la auditoría, así como el programa detallado de la investigación.

La investigación preliminar comenzara con una visita a la organización, al área de informática y a los equipos de cómputo y solicitar una serie de documentos. Se analizara el estado general del departamento o área, su situación dentro de la organización.

CAPITULO 2. AUDITORÍA DE LA FUNCIÓN INFORMÁTICA

2.1 Recopilación de la Información Organizacional

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

2.1.1 Estructura Organizacional

Para su evaluación se deberá solicitar el manual de organización del área, el cual debe contener como mínimo: organigrama con jerarquías, funciones, objetivos y políticas, análisis, descripción y evaluación de puestos, manual de procedimientos y normas e instructivo de trabajo o guías de actividad.

2.1.2 Situación de los Recursos Humanos

Se deberá obtener información sobre los siguientes aspectos desempeño y comportamiento, condiciones de trabajo, ambiente, organización en el trabajo, desarrollo y motivación, capacitación y supervisión, del personal del área, para lo cual se puede utilizar la tabla de recursos humanos y la tabla de proyección de recursos humanos.

2.1.3 Entrevistas con el Personal de Informática

Estas entrevistas servirán para determinar el grado de cumplimiento de la estructura organizacional administrativa, el grado de cumplimiento de las políticas y procedimientos administrativos, satisfacción e insatisfacción, capacitación y observaciones generales.

2.1.4 Situación Presupuestal y Financiera

Se obtendrá información presupuestal y financiera del departamento, así como el número de equipos y características para analizar su situación desde un punto de vista económico.

2.2 Principales Documentos que se Necesitan

2.2.1 Estudio de Viabilidad

Consiste en determinar si el equipo de cómputo disponible puede resolver o mejorar un determinado procedimiento y, saber cuál sería la mejor alternativa.

2.2.2 Plan de Cambios, Modificaciones y Actualización

Especifica las metas y actividades que deben realizar para lograr los cambios y modificaciones, su independencia, tiempos, responsables y restricciones, cuando la organización toma la decisión de hacer cambios sustanciales de hardware, software, comunicaciones o equipos periféricos.

2.2.3 Plan Estratégico o Maestro

El plan estratégico deberá contener los objetivos, metas y actividades generales a realizar durante los siguientes años, incluirá nuevos sistemas que se pretenda implementar. Este plan puede comprender cuatro subplanes:

- A) El plan estratégico de organización.
- B) El plan estratégico de sistemas de información.
- C) El plan de requerimientos
- D) El plan de aplicaciones de sistemas de información

2.2.4 Plan de Proyectos

Plan básico para desarrollar determinado sistema, conforme a las metas y objetivos de la organización y con los señalados en el plan estratégico.

2.2.5 Plan de Seguridad

Este plan permitirá eliminar en lo posible la ocurrencia de un desastre o de pérdida por causas internas o externas a la organización. Deberá considerarse plan de seguros, así como de recuperación en caso de que ocurra un desastre la instalación se ponga en funcionamiento en el menor tiempo posible y con el menor impacto para la organización.

2.3 Funciones y Objetivos

Las funciones son las principales actividades a desarrollar por el área de informática, estas definen de un organismo a otro.

Los objetivos son los motivos prioritarios por los cuales existe el área de informática.

CAPITULO 3. EVALUACIÓN DE LOS SISTEMAS

3.1. Evaluación de los Sistemas

Deberá ser evaluada con mucho detalle, para lo se debe revisar e identificar si existen sistemas entrelazados como un todo o bien si existen programas aislados, así como evaluar si existe un plan estratégico para la elaboración de los sistemas o si se están elaborando sin el adecuado señalamiento de necesidades y de objetivos.

El plan estratégico de desarrollo debe establecer las nuevas aplicaciones y recursos que proporcionará la dirección de informática y la arquitectura en la que están fundamentados. En lo referente a consultar los usuarios, el plan estratégico debe definir los requerimientos de la información de la organización.

El proceso de planeación de sistemas debe asegurarse de que todos los recursos requeridos estén claramente identificados en el plan de desarrollo de aplicaciones y datos.

Para identificar los problemas de los sistemas primero se deben detectar los síntomas, los cuales son un reflejo del área problemática; y después de analizar los síntomas, se podrán definir y detectar las causas.

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

3.2 Evaluación del Análisis

Dentro de la evaluación del análisis también se deben evaluar las políticas, procedimientos y normas que se tienen para llevar a cabo el análisis. Se debe evaluar la planeación de las aplicaciones que pueden provenir de cuatro principales:

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

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

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

Revisión de la situación en que se encuentran los manuales de análisis y si están de acorde con las necesidades de la organización. Esto quiere decir que los sistemas y su documentación deben estar acordes con las características y necesidades de la organización.

Evaluar los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, archivos almacenados, su uso y su relación con otros archivos y sistemas, su referencia de acceso, conservación, seguridad y control, la documentación propuesta, las entradas y salidas del sistema y documentos fuente.

Evaluar la obtención de datos sobre la operación, flujo, nivel de jerarquía de la información que se tendrá a través del sistema así como sus límites e interfaces con otros sistemas. Es decir comparar los objetivos de los sistemas desarrollados con las operaciones actuales, para ver si el estudio de la ejecución deseada corresponde al actual.

3.3 Evaluación del Diseño Lógico del Sistema

En esta etapa se analizarán las especificaciones del sistema, al realizar el análisis debemos compararlo con lo que realmente se está obteniendo, es decir evaluar cómo fue planeado y lo que realmente se está obteniendo.

3.4 Programas de Desarrollo

En esta parte incluye software que es usado por el personal que ha tenido entrenamiento y experiencia; por ejemplo:

Lenguajes de programación:

Lenguaje de máquina

Ensambladores

De tercera generación

De cuarta generación

CASE (computer aided software engineering).

Programación orientada a objetos.

Al utilizar un determinado software se evalúa lo siguiente:

Interfaces de usuario gráfico

Enlace de objetos en los sistemas de información

Capacidad de trabajar en multi-plataformas

Capacidad de trabajar en redes

Licencias y tipo

Transportable

Compatible con otro software y con periféricos

Fácil de usar

Grado de sofisticación

Capacidad de utilización en red

De fácil instalación

Demanda de hardware

Requerimiento de memoria

Costo

Seguridad y confidencialidad

3.4.1 Bases de Datos

En las bases de datos de debe evaluar:

La independencia de los datos; es decir, que la falta de independencia significa que cada vez que un archivo es cambiado, todo programa que acceda a ese archivo debe ser cambiado.

Redundancia de los datos es toda aquella duplicidad de datos.

Consistencia de los datos;

Los componentes a evaluar dentro de una base de datos son:

Diccionario/directorio de datos,

Lenguajes de datos (DDL, DML),

Monitoreo de teleproceso,

Herramientas de desarrollo de aplicaciones,

Software de seguridad,

Sistemas de almacenamiento, respaldo y recuperación,

Reporteadores,

Query languages (SQL, QBE),

Bases de datos de multiplataformas,

Web Server Software.

Un administrador de Bases de Datos tiene la función de planear, diseñar, organizar, operar, entrenar, así como dar soporte a los usuarios, seguridad y mantenimiento.

3.5 Comunicación

Es un factor importante evaluarlo, y este dependerá de la velocidad y capacidad de transmisión, ya que está directamente relacionado con el costo (cable trenzado, cable coaxial, fibra óptica, etc.). Los componentes a evaluar son:

Servidor y huésped

Terminal o estación de trabajo

Convertidores de protocolos

Módem

Equipo de conexión de terminales

Modo de comunicación

Medio de comunicación

Topología de redes

Tipo de redes

3.5.1 Ruido, Redundancia, Entropía

Ruido todo aquello que interfiere en una adecuada comunicación, ejemplo; el error en una captura, una pantalla demasiado llena de información y poco entendible o un reporte inadecuado, ya que impiden una buena comunicación con la información.

Redundancia es la duplicidad que tiene un sistema con la finalidad de que, en caso de que exista ruido, permita que la información llegue al receptor en forma adecuada.

Entropía, es el máximo aprovechamiento de la energía, ejemplo: la interconexión de sistemas.

3.6 Evaluación del Desarrollo del Sistema

En esta etapa se deberán auditar los programas, su diseño, lenguaje utilizado, interconexión entre los programas y las características del hardware empleado para el desarrollo del sistema.

3.7 Sistemas distribuidos, Internet, Comunicación entre oficinas

3.7.1 Control de Proyectos

Para poder controlar el avance de los sistemas, se recomienda utilizar la técnica de administración por proyectos para su adecuado control. Para tener una buena administración por proyectos se requiere que el analista o el programador y su jefe inmediato elaboren un plan de trabajo en el cual se especifiquen actividades, metas, personal participante y tiempos. Este plan deberá ser revisado periódicamente para evaluar el avance respecto a lo programada.

La planeación de proyectos incluye fechas predefinidas de terminación de cada tarea, así como, fechas calendarizadas para reuniones de revisión, las cuales tendrán diferentes niveles de detalle.

3.8 Control de Diseño de Sistemas y Programación

El propósito es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, para que sea de utilidad al usuario para su manejo, operación y aceptación.

Las revisiones se llevan a cabo en forma paralela desde el análisis hasta la programación con los siguientes objetivos:

Etapa de análisis y definición del problema. Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

Etapa de estudio de factibilidad. Elaboración del costo/beneficio del sistema, desarrollando el modelo lógico, hasta llegar a la decisión de elaborarlo o rechazarlo, incluyendo el estudio de factibilidad técnico y las recomendaciones.

Etapa de Diseño. Descubrir errores, debilidades, omisiones antes de iniciar la programación.

Etapa de programación. Buscar la claridad, modularidad, y verificar con base en las especificaciones.

Las pruebas del sistema tratan de garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando datos estadísticos, transacciones, reportes, archivos, registrando las fallas que pudieran ocurrir y realizando los ajustes necesarios. Estas pruebas pueden ser agrupadas en módulos, programas y sistema total.

3.9 Instructivos de Operación

Se evalúan para evitar que los programadores tengan acceso a los sistemas en operación.

3.10 Forma de Implantación

Esto comprende prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento de los responsables del sistema, considerando los siguientes aspectos:

- Indicar cuales puntos se toman en cuenta para la prueba de un sistema

- Análisis de la forma en que se van a cargar inicialmente los datos del sistema, lo cual puede ser por captura o transferencia de información.

3.11 Equipo y Facilidades de Programación

La selección de la configuración de un sistema de cómputo incluye la interacción de numerosas y complejas decisiones de carácter técnico. El impacto en el rendimiento de un sistema debido a cambios de trascendentales en el sistema operativo o en el equipo, puede ser determinado por medio de un paquete de pruebas que haya sido elaborado para este fin en la dirección informática.

3.12 Entrevistas a Usuarios

El objetivo es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora y de los sistemas en operación. Deberán hacerse de preferencia a todos los usuarios o en forma aleatoria, en cuanto al uso del equipo.

Para que un sistema cumpla con los requerimientos del usuario, se necesita una comunicación completa entre usuario y el responsable del desarrollo del sistema.

**CAPITULO 4. EVALUACIÓN DEL PROCESAMIENTO DE
DATOS Y EQUIPO DE CÓMPUTO**

4.1 Controles

Los datos son muy valiosos en las organizaciones y también necesitan ser controlados y auditados cuidadosamente, por lo que hay que tener presente:

La responsabilidad de los datos es compartida conjuntamente por alguna función determinada de la organización y la dirección de informática.

Un problema frecuente que se origina es la duplicidad de datos y consiste en poder determinar los propietarios o usuarios posibles y la responsabilidad de su actualización y consistencia.

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

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

Entre las políticas de operación de las computadoras se encuentran las siguientes:

4.1.1 Políticas de Respaldo

Los respaldos de información deben realizarse mensual, semanal o diario considerando lo siguiente:

Contar con políticas por escrito para efectuar los respaldos según el periodo requerido.

Los medios magnéticos no deben estar almacenados en un mismo lugar.

Tener acceso restringido al área de almacenamiento de los medios magnéticos.

Identificar las cintas por fecha, concepto y consecutivo.

4.1.2 Políticas y Procedimientos

Todos los procedimientos de las diversas actividades deberán estar documentadas, al igual que las normas y políticas, se manifestaran por escrito en manuales de operación.

4.1.3 Políticas de Bitácoras

Deben existir bitácoras de operación en las que se registren los procesos realizados, resultados de su ejecución, concurrencia de errores, los procesos ejecutados en el equipo y la manera en que concluyeron.

4.1.4 Control de las Licencias de Software

Contar con un inventario actualizado de las licencias de software, que asegure la paquetería y software sea legal y esté amparada por una licencia, para evitar posibles problemas legales por pago de derechos de uso y explotación del software.

4.2 Control de Datos Fuente y Manejo de Cifras de Control

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al; suprimir u omitir datos, adicionar datos, alterar datos y duplicar procesos.

Es de muy importante en caso de equipos de cómputo que cuentan con sistemas en línea, en los que el usuario es el responsable de la captura y modificación de la información al tener un adecuado control con señalamiento de responsables de datos, con claves de acceso de acuerdo con niveles.

El primer nivel es el que únicamente puede hacer consultas.

Segundo nivel es que puede hacer captura, modificaciones y consultas.

Tercer nivel es el que solo puede hacer todo lo anterior y además realizar bajas.

4.3 Control de Operación

Los instructivos de operación proporcionan al operador información sobre los procedimientos que debe seguir en situaciones normales y anormales en el procesamiento, y si la documentación es incompleta o inadecuada lo obliga o suspender o improvisar los procesos mientras investiga lo conducente, generando probablemente errores, reprocesos, desperdicio de tiempo de máquina.

4.4 Control de Asignación de Trabajo

Se relaciona con el control de las operaciones de la computadora en términos de la eficiencia y satisfacción del usuario. Se evalúan los procedimientos de programación de cargas máquina para determinar si se ha considerado disminuir los picos de los procesos, originados por cierres mensuales y balancear las cargas de trabajo de bath y línea.

4.5 Control de Medios de Almacenamiento Masivo

La dirección de informática deberá tener perfectamente protegidos estos dispositivos de almacenamiento y mantener registros sistemáticos de la utilización de los archivos, de tal forma que sirvan de base a los programas de limpieza, principalmente en el caso de las cintas. Esto incluye la identificación de los carretes para evitar la utilización errónea o destrucción.

4.6 Control de Mantenimiento

Al evaluar el mantenimiento primero debemos analizar cuál es el que más conviene, y en segundo lugar revisar los contratos con detalle que las cláusulas estén bien definidas, que no exista subjetividad y que exista penalización en caso de incumplimiento. Para poder exigir el cumplimiento del contrato se debe tener un estricto control sobre las fallas, frecuencia y el tiempo de reparación.

4.7 Orden en el Centro de Cómputo

Una dirección de informática debe contar con reglas, disposiciones o un reglamento relacionado con el orden y cuidado del área de máquinas para que este bien administrada.

4.8 Configuración del Sistema de Cómputo

Evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de la instalación y revisar las políticas seguidas por la unidad de informática, esto va orientado a:

Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo.

Evaluar las posibilidades modificar el equipo para reducir el costo o el tiempo de proceso.

Evaluar la utilización de los diferentes dispositivos periféricos

4.9 Productividad

Evaluar la eficiencia con que opera el área de captación y producción.

4.10 Equipos de Cómputo

No contar con políticas y estándares de adquisición o renta de equipos de cómputo, cada área o empleado puede adquirir diferentes equipos, el cual puede no ser compatible o bien el conocimiento y entrenamiento requerirá de mayor tiempo y costo. El mantenimiento es otro factor que puede incrementarse en caso de no tener compatibilidad de equipos.

CAPITULO 5. EVALUACION DE LA SEGURIDAD

5.1 Seguridad Lógica y Confidencialidad

Se encarga de controlar y salvaguardar la integridad de la información almacenada en las computadoras, generada por los sistemas, software de desarrollo y programas en aplicación; identifica individualmente a cada usuario y restringe el acceso a datos, a los programas, a redes y terminales. La violación o falta de seguridad lógica puede originar consecuencias como:

Cambio de datos antes o cuando se le da entrada a la computadora.

Copias de programas y/o información

Código oculto en un programa

Entrada de virus

El tipo de seguridad puede comenzar desde la simple llave de acceso, hasta sistemas más complejos, pero hay que evaluar que entre más complejos sean los dispositivos de seguridad más costosos resultan.

Otro método eficaz para proteger sistemas de computación es el software de control de acceso, es decir, son paquetes de control de acceso que protegen contra el acceso no autorizado.

Un sistema integral de seguridad debe comprender:

Elementos administrativos

Definición de una política de seguridad

Organización y división de responsabilidades

5.2 Seguridad Lógica

Esta seguridad está definida por el grado de actuación que puede tener un usuario en un sistema, en una base de datos o en una red. Existen varios tipos de usuarios:

Propietario. Es el dueño y responsable de la información puede realizar cualquier función.

Administrador. Únicamente puede actualizar o modificar el software con autorización.

Usuario principal. Puede realizar modificación, cambio, lectura y utilización de los datos.

Usuario de consulta. Solo puede leer la información pero no modificarla.

Usuario de explotación. Puede leer y utilizar la información para generación de reportes.

Usuario de auditoria. Utiliza y rastrea información dentro del sistema con fines auditables.

La seguridad lógica abarca estas áreas:

Rutas de acceso

Claves de acceso

Software de control de acceso

Encriptamiento

5.2.1 Rutas de Acceso

Las rutas de acceso nos sirven para identificar puntos de control que pueden ser usados para proteger los datos en el sistema. Estas rutas de acceso se encuentran en cada sistema de información y es la trayectoria seguida en el momento de acceder al sistema.

Tipos de restricciones:

Solo lectura

Solo consulta

Lectura y consulta

Lectura, escritura, para crear, actualizar, borrar, ejecutar o copiar.

5.2.2 Claves de Acceso

Métodos de identificación para los usuarios:

Llaves de acceso, código o password

Credencial con banda magnética

Validación por características

Password, código o llaves de acceso. Son usadas para controlar el acceso a la computadora, a sus recursos, tienen definido el nivel de acceso o funciones específicas.

Características de las llaves de acceso:

Válida y verificada por el sistema

Longitud adecuada

No debe ser desplegada al ser tecleada

Debe ser encriptada

Prohibir el uso de nombres, palabras o caracteres fáciles de identificar

Credenciales con banda magnética. Son como las bancarias, además de que contenga fotografía y firma.

Validación por características. Consiste en la verificación y reconocimiento de la identidad de las personas, utilizando características propias como:

Huellas dactilares

Retina

Geometría de la mano

Firma

Voz

5.2.3 Software de Control de Acceso

Programa diseñado para permitir el manejo y control de acceso a recursos como; programas de librerías, datos, programas de aplicación, módulos de funciones, utilerías, diccionario de datos, archivos, programas y comunicaciones.

Este software almacena y analiza los eventos realizados y el uso de los recursos, a través de las siguientes funciones:

Definición del usuario

Definición de las funciones del usuario después de acceder al sistema

Establecimiento de auditoría a través del uso del sistema

5.2.4 Encriptamiento

Encriptar es la transformación de datos a una forma en que no sea posible leerla por cualquier persona. El propósito es asegurar la privacidad y mantener la información alejada del personal no autorizado, aun de aquellos que la pueden ver en forma encriptada.

5.3 Seguridad en el Personal

La integridad, estabilidad y lealtad del personal dependen en gran medida en un buen centro de cómputo. Por lo que se deben considerar valores sociales y su estabilidad en general, mediante exámenes psicológicos y médicos, así como considerar antecedentes de trabajo.

Deberá contarse con políticas de vacaciones, reemplazo y de rotación de personal, para evitar la dependencia o la posibilidad de fraudes.

5.4 Seguridad Física

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

5.5 Ubicación y Construcción del Centro de Cómputo

La ubicación del centro de cómputo dentro de la organización deberá ser en un lugar poco visible, con poco flujo de personas así como de personal, ya que puede ser vulnerable al sabotaje o terrorismo.

El tipo de construcción se debe tener precaución con los materiales altamente inflamables, que despiden humos tóxicos o paredes que no quedan perfectamente selladas y despiden polvo. También debe considerarse la orientación, por ejemplo a lugares que todo el día les está dando el sol y evitar ventanales grandes.

Las dimensiones se determinaran por el número de componentes del sistema, espacio para cada unidad, para su mantenimiento y área de operación.

5.6 Piso Elevado o Cámara Plena

Actualmente este tipo de requerimiento ya no es muy común, ya que este es utilizado en centros de cómputo con macro-computadoras. Este piso elevado debe ser capaz de soportar una carga uniforme, de acuerdo con las especificaciones del proveedor, así como capacidad de soportar unidades adicionales según el potencial de crecimiento.

5.7 Aire Acondicionado

Este dispositivo dependerá del tipo de computadoras que se utilicen y del lugar donde está instalado, se debe verificar con el proveedor la temperatura mínima y máxima, así como la humedad en que deberán trabajar los equipos.

5.8 Instalación Eléctrica y Suministro de Energía

Es altamente recomendable que los cables del sistema eléctrico, para el equipo de cómputo cuenten con tierra física y sistema de corriente continua (no-break), así como

aislador con contactos independientes e identificados (positivo, negativo y tierra física). Las conexiones deben estar independientes para los equipos de cómputo. En cuanto a la tierra física debe ser instalada de acuerdo con las especificaciones del proveedor y deberá contar con protección contra fauna nociva en los cables del sistema eléctrico y comunicaciones.

5.8.1 Reguladores

Dispositivo electrónico que reduce el riesgo de accidentes por los cambios de corriente, para asegurar que el regulador actuara en una sobrecarga en bajos niveles debe tener un sistema no interrumpido.

Un sistema no interrumpido (UPS) consiste en un generador de batería o de gas, que hace interface entre la energía eléctrica y el dispositivo de entrada de energía a la computadora, la cual puede ser de horas o de algunos minutos, y se puede permitir respaldar la información.

5.9 Seguridad contra Desastres Provocados por Agua

El centro de cómputo no debe ubicarse en planta baja o sótanos, de preferencia en partes altas de una estructura de varios pisos.

5.10 Seguridad de Autorización de Accesos

Los controles de acceso deben ser estrictos durante todo el día, esto incluye a todo el personal de la organización, en especial durante los descansos y cambios de turno.

5.11 Detección de Humo y Fuego, Extintores

Los detectores de humo y calor se deben instalar en las áreas de oficinas, incluyendo el depósito de papelería y el perímetro físico de las instalaciones.

Los extintores portátiles de CO, se deben colocar en lugares estratégicos. El equipo para poder respirar debe estar a la mano incluso para el uso de los bomberos en caso de incendio. Se debe señalar las salidas de emergencia.

5.12 Temperatura y Humedad

Se recomienda la instalación de instrumentos registradores de temperaturas y humedad, con la finalidad de proveer un continuo registro de las condiciones ambientales en el área.

5.13 Seguridad en Contra de Virus

Para evitar que los virus se diseminen por todo el sistema o por las redes se debe:

- Utilizar paquetes y programas originales
- Solo permitir el acceso a la parte del sistema autorizado para cada usuario
- Evitar que todos los usuarios puedan navegar por todos los sistemas
- Limitar la programación y controlarla adecuadamente

Se debe contar con vacunas contra virus; otra forma de protegerse es a través de analizadores de virus.

CAPITULO 6. APLICACIÓN DEL CASO

Se aplicaron cuestionarios para la evaluación de cada fase de la auditoría informática, de preguntas con respuesta cerrada para facilitar la interpretación de los datos, al personal informático que se encuentra en cada departamento que constituyen a la jurisdicción, siendo 28 elementos y un tamaño de muestra de 21, con un margen de error del 10 %.

6.1 MARCO DE REFERENCIA

La Jurisdicción Sanitaria Pátzcuaro, es la unidad técnico-administrativa desconcentrada de la Secretaria de Salud de Michoacán, a la cual se asignan recursos para otorgar atención médica a población abierta, Oportunidades, Seguro Popular y para realizar acciones de regulación sanitaria, delegándole facultades para conducir las acciones del sector en su área de influencia. Ubicada en la Av., Lázaro Cárdenas 509, teléfonos 4343420712, 4343421488 y fax 4343421878, correo electrónico js4direccion@salud.michocan.gob.mx.

6.1.1 Descripción Estratégica de la Organización (Giro, Misión, Visión, Organigrama)

Giro

Otorgar servicios de atención preventiva y promoción a la salud de la población de responsabilidad.

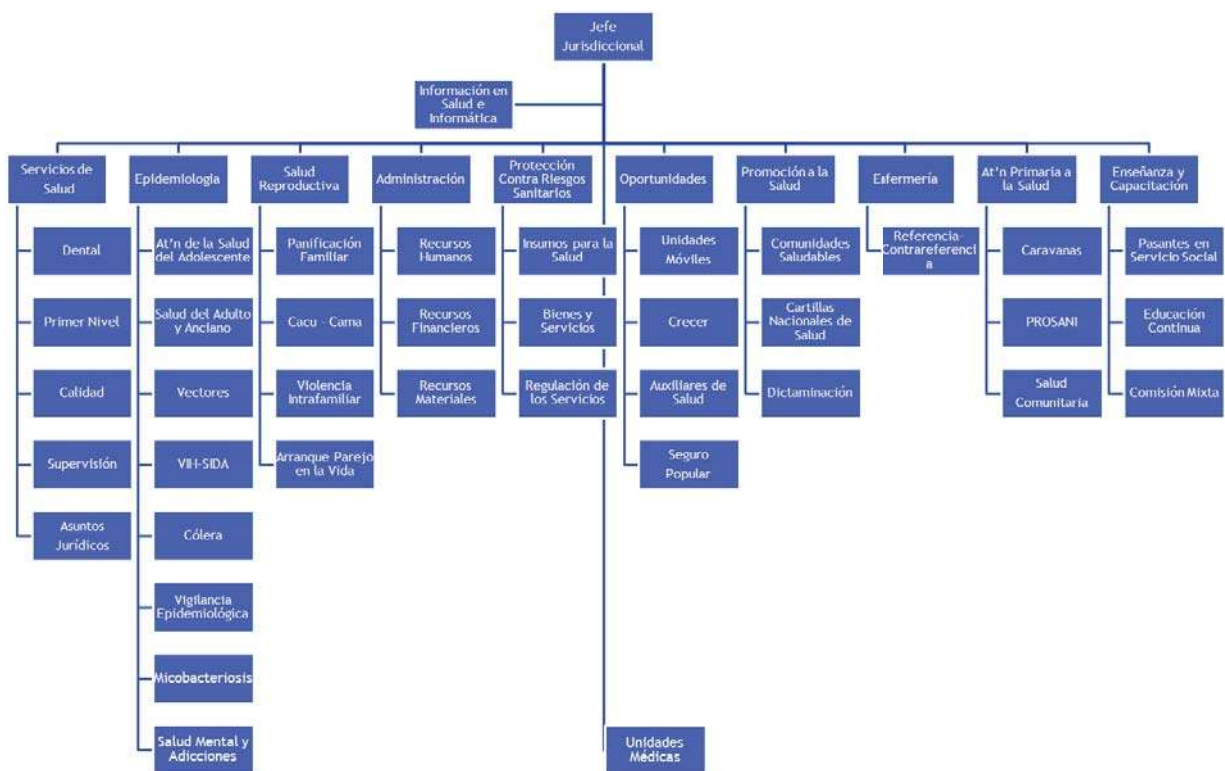
Misión

Contribuir en su desarrollo humano, justo, incluyente y sustentable, mediante la promoción de la salud como objetivo social compartido y el acceso universal a servicios de salud integrales, de alta calidad, que satisfagan las necesidades y respondan a las expectativas de la población, al tiempo que ofrecen oportunidades de avance profesional a los prestadores de servicios, en el marco de un financiamiento equitativo, el uso honesto, transparente y eficiente de los recursos y una amplia participación ciudadana.

Visión

Formación de un sistema de salud universal, solidaria, plural, eficiente y de alta calidad, atendiendo a las necesidades de la población de responsabilidad, con una amplia participación ciudadana.

Organigrama Operacional



6.1.2 Antecedentes

6.2 AUDITORIA DE LA FUNCION INFORMATICA

6.2.1 ALCANCE Y OBJETIVOS DE AREA

Organización de la dirección de Informática
Plan estratégico
Análisis de puestos y evaluación del personal
Evaluar los recursos financieros y materiales
Programas y procedimientos
Normatividad
Funciones, objetivos.

6.2.2 CUESTIONARIO

Preguntas	SI	NO
1. ¿Es adecuada la estructura orgánica para las disposiciones jurídicas vigentes?		
2. ¿El área de informática cuenta con planes o programas y procedimientos de trabajo?		
3. ¿Sabe si están establecidas las funciones del área de informática?		
4. ¿Sabe si existe presupuesto financiero para cumplir con las funciones?		
5. ¿Están establecidos los objetivos del área de informática?		
6. ¿Es suficiente el personal para cumplir con las funciones asignadas?		
7. ¿Se requieren más áreas para llevar a cabo las funciones del área de informática?		
8. ¿Existen un programa de evaluación para el personal informático?		
9. ¿Se cuenta con el equipo, material y mobiliario para desarrollar el trabajo?		
10. ¿Se considera al personal informático para la toma de decisiones de la jurisdicción, en cuanto a su competencia?		
11. ¿Se realiza un análisis de la planeación estratégica?		

12. ¿Cuenta con un programa de capacitación para el personal informático?		
13. ¿Existen controles administrativos sobre los recursos informáticos?		
14. ¿Consideras que el área de informática debería estar como un departamento independiente dentro de la jurisdicción?		

6.2.3 HALLAZGOS ENCONTRADOS

- El área de informática actualmente funciona como área de soporte y asesoría para los demás departamentos, ya que existe personal con conocimientos básicos en dichos departamentos.
- No cuenta con planes y programas de trabajo, objetivos y funciones bien definidas ya que no han sido requeridos por el jefe inmediato, ni enviados o solicitados por el nivel estatal.
- Se identifica que algunas actividades y toma de decisiones referentes al equipo de cómputo y sistemas automatizados, se llegan a ejecutar sin conocimiento y opinión del responsable del área, se toma la decisión por parte del coordinador o responsable del programa o departamento.
- No se ha realizado supervisión al área de informática durante varios años. No se cuenta con recursos financieros, materiales o presupuesto propios, para ejecución y cumplimiento de sus funciones. Existe presupuesto informático pero se encuentra establecido o integrado en el presupuesto de cada programa de salud, esto hace que el coordinador del programa y administrador apliquen ese presupuesto de acuerdo a las necesidades, en ocasiones no es destinado correctamente.
- El área de informática por disposiciones legales no está estructurada como un centro de cómputo, sino como un enlace de informática conjuntamente con el área de Información en Salud.
- Se realizan adquisiciones o compras de equipos de cómputo sin un proceso adecuado ya que la decisión se lleva a cabo entre el coordinador del programa y el administrador.

- En cuanto al responsable lleva a cabo otras funciones de estadística y también es el que realiza las funciones informáticas y el resto del personal está destinado como apoyo.
- Otro de los factores deficientes es la remuneración del personal informático que no es apego con el binomio código-función.

6.2.4 CONCLUSIONES

Considero que el área de informática se encuentra aislada ya que no es considerada para la toma de decisiones de la jurisdicción, otro de los puntos que repercuten en esto es que no se asigna recurso financiero por las autoridades estatales.

Cuenta con varias deficiencias en cuanto a organización por diferentes causas, no se ha solicitado elaboración de programas y planes de trabajo, reporte de actividades y necesidades para cumplir con las funciones.

El área de informática se encuentra centralizada ya que se ubica en la gerencia general como asesoría y soporte lo cual no permite contar con recursos disponibles para adquisición y cumplimiento de actividades encomendadas.

6.2.5 RECOMENDACIONES

- ✓ Descentralizar el departamento o área de informática de forma independiente a la jefatura.
- ✓ Establecer funciones y objetivos del área de informática.
- ✓ Proponer una partida presupuestal de forma propia para informática, al nivel local y estatal.
- ✓ Dar a conocer a los coordinadores de programas de salud y usuarios, la importancia de las responsabilidades del área de informática.
- ✓ Establecer personal responsable y de apoyo para el área, para cubrir las necesidades de índole informático.

- ✓ Aplicar el recurso financiero integrado en los programas de forma adecuada, con la participación de informática.
- ✓ Aplicar estímulos monetarios al personal informático de acuerdo con las condiciones generales de trabajo.
- ✓ Considerar el área de informática como parte esencial de la jurisdicción y no únicamente como de apoyo.

6.3 EVALUACION DE LOS SISTEMAS

6.3.1 ALCANCE Y OBJETIVOS DE AREA

Identificar si se cuentan con los sistemas necesarios para cumplir con sus funciones

Importancia de la evaluación del diseño lógico de un sistema y su desarrollo

Características principales de control de proyectos, para el desarrollo de un sistema

Contenido que debe tener los instructivos de operación de los sistemas

Procesos que se deben realizar para iniciar la operación de un sistema

6.3.2 CUESTIONARIO

Preguntas	SI	NO
1. ¿Se desarrollan sistemas de información para cumplir con las funciones?		
2. ¿Se proporciona capacitación para el manejo de los Sistemas de Información implementados?		
3. ¿Se cuenta con los manuales de operación de los sistemas de información?		
4. ¿Los Sistemas de Información cumplen con los requerimientos?		
5. ¿Se han realizado actualizaciones?		
6. ¿Maneja licencias originales de los Sistemas Operativos?		
7. ¿Existen las pólizas de seguro de los sistemas?		
8. ¿Cuenta con software ofimática o comercial?		
9. ¿Cuenta con recurso financiero para adquisición de Sistemas o Programas?		
10. ¿Dispone y son vigentes los seguros del Software?		
11. ¿Existe un programa de mantenimiento preventivo a los Sistemas de Información?		
12. ¿Son compatibles los Sistemas de Información con el Software preinstalado?		
13. ¿Cuenta con contratos de compra y soporte del Software?		
14. ¿Cuenta con un directorio del proveedor de soporte de Software?		

15. ¿Existen copias de respaldo de los Sistemas de Información?		
16. ¿Cuentan con llaves de acceso a los Sistemas de información?		
17. ¿La configuración de los Sistemas es la adecuada?		
18. ¿Se manejan Sistemas de distribución libre?		
19. ¿Existe inventario del Software utilizado?		
20. ¿Registra el número de fallas de los sistemas?		

6.3.3 HALLAZGOS ENCONTRADOS

- No se desarrollan sistemas ya que son implementados por el nivel estatal o federal dependiendo del departamento y del programa de salud. Sin embargo, los usuarios y coordinadores de programas de salud han identificado la necesidad del desarrollo de pequeños programas o herramientas automatizadas para el proceso de algunas actividades.
- No se cuenta con un presupuesto o contratos de compra de Software. Lo que implica la utilización e instalación de software ofimática pirata, algunas versiones de sistemas operativos y antivirales.
- Los sistemas utilizados son para la captura de datos y son enviados por el nivel estatal o federal. Los sistemas estatales no llegan a cumplir con los requerimientos de funcionalidad para los propósitos del programa de salud.
- Se llega solicitar el desarrollo de aplicaciones sencillas para la ejecución de algún programa en salud, pero por razones de tiempos y otras actividades no se pueden llevar a cabo.
- En cuanto a la comunicación o transferencia de datos intranet e internet, se cuenta con una red de área local deficiente sin apego a estándares de instalación, debido a la falta de recurso para la adquisición de dispositivos y periféricos.
- No se dispone en su mayoría de los instructivos de operación de los sistemas. No se llevan a cabo actualizaciones a la par con la implementación de los programas de salud.
- Existen sistemas y programas, con demasiada saturación de información en sus pantallas de captura.

- Falta de capacitación y actualización en la utilización de aplicaciones y software.

6.3.4 CONCLUSIONES

Actualmente el nivel jerárquico que tiene el área de informática no cuenta con el desarrollo y diseño de sistemas, por lo cual únicamente sus funciones son de operadores de sistemas automatizados.

Sin embargo el 75% de los usuarios informáticos no tiene el suficiente nivel de conocimiento y funcionalidad de los sistemas, para lo cual se requiere capacitaciones.

Una adecuada arquitectura en la instalación de una red local, garantizara calidad de la información enviada por este medio.

6.3.5 RECOMENDACIONES

- ✓ Solicitar contratos de compra del software así como un directorio del proveedor al nivel estatal.
- ✓ Llevar un control del uso de software comercial.
- ✓ Adquirir software antivirus original para disminuir las incidencias de contagios o pérdidas de información.
- ✓ Proponer al nivel estatal las necesidades de creación de aplicaciones o herramientas solicitadas.
- ✓ Solicitar la instalación adecuada de la red local ya que la mayoría de la captura de datos se realiza a través de internet.
- ✓ Solicitar e Integrar los instructivos de operación de sistemas, etiquetarlos y resguardarlos para su consulta.

6.4 EVALUACION DEL PROCESO DE DATOS Y DE LOS EQUIPOS DE CÓMPUTO

6.4.1 ALCANCE Y OBJETIVOS DE AREA

Controles que se deben ejercer sobre los datos

Reglas relativas de orden y control en el centro de cómputo

Grado de eficiencia del sistema de operación

6.4.2 CUESTIONARIO

Preguntas	SI	NO
1. ¿Sabe si existe un sistema manejador de bases de datos?		
2. ¿Se implementan procedimientos de captura de datos?		
3. ¿Existe un registro de control de la información capturada?		
4. ¿Se verifica la calidad de la información recibida para la captura?		
5. ¿Existe algún proceso que indique que hacer con la información incorrecta?		
6. ¿Existe algún área segura para el resguardo de la información capturada?		
7. ¿Se realizan reportes sistemáticos de la información capturada?		
8. ¿Se evalúa la productividad de la información capturada por persona?		
9. ¿Existe un inventario del equipo de cómputo?		
10. ¿El inventario esta actualizado?		
11. ¿Los equipos de cómputo son adquiridos por el área de informática para su distribución en los diferentes departamentos?		
12. ¿Están identificados los equipos de cómputo?		
13. ¿Se cuentan con seguros de póliza de los equipos de cómputo?		
14. ¿Existe un contrato de mantenimiento de los equipos de cómputo?		
15. ¿Cuenta con material para realizar mantenimiento de limpieza de los equipos?		
16. ¿Se hace un uso racional de los equipos de cómputo?		

17. ¿Los equipos de cómputo cumplen con las necesidades del trabajo?		
18. ¿Existe un inventario de los componentes (D.D. memoria RAM, DVD, CD) de los equipos de cómputo?		
19. ¿Es adecuada la distribución de los equipos de cómputo?		
20. ¿La instalación y suministro eléctrico es la adecuada para la operación de los equipos de cómputo?		
21. ¿Existe reglas del manejo adecuado de los equipos de cómputo?		
22. ¿La configuración de los equipos de cómputo es la adecuada?		
23. ¿Cuenta con un registro del equipo de cómputo obsoleto o en desuso?		

6.4.3 HALLAZGOS ENCONTRADOS

- No se cuenta con sistema manejador de bases de datos, ya que se manejan sistemas locales para la captura de la información por el personal informático y en algunos sistemas la información es captura en línea a través de internet que se almacena en servidores ubicados en oficinas centrales a nivel nacional.
- Las bases de datos manejadas por los capturistas están diseñadas en Microsoft Access, MySQL y Visual Fox Pro, para la captura de información.
- Como algunos programas no cumplen con los requerimientos de funcionalidad, los usuarios optan por manipular los datos directamente en la base de datos para la generación de reportes o actualización de algunos datos.
- No se lleva a cabo políticas de respaldos de información, los procedimientos de captura no cuenta con criterios bien definidos.
- Referente a la captura de datos no se implementa ningún registro de control en algún formato, en ningún departamento. Tampoco se evalúa la productividad de la captura.
- No se cuenta con un inventario actualizado de los equipos de cómputo ya que parte de estos es enviado directamente al departamento que corresponde del nivel estatal y no se informa debidamente.
- La adquisición de equipo de cómputo o dispositivos se realiza sin un adecuado proceso, ya que optan por hacer compras de equipos ensamblados.

- No existe un programa de mantenimiento preventivo y correctivo de los equipos de cómputo a nivel jurisdiccional ya que no se cuenta con presupuesto.
- En cuanto a las pólizas de garantía tampoco se dispone de ellos ya que estos se encuentran en el departamento de recursos materiales a nivel estatal.
- La instalación del cableado de la red local, se encuentra expuesto a la intemperie externa como internamente en cada una de los departamentos

6.4.4 CONCLUSIONES

La implementación de registros de control para la captura de datos, permitirá la identificación de subregistro o duplicidad de datos.

No se cuenta con una comunicación entre departamento estatal que realiza la adquisición y distribución de los equipos de cómputo con el área de informática jurisdiccional.

No se lleva a cabo un control del equipo de cómputo obsoleto, el departamento de almacén realiza la baja del equipo pero no entrega ninguna copia o información para informática.

Los dispositivos periféricos como impresoras, no llegan a ser utilizadas adecuadamente, ya que al momento del atasco de papel u objetos extraños, el usuario por desconocimiento los daña al intentar quitar el atasco.

Contar con un inventario de reguladores o No-Breaks es indispensable.

La inexistencia de programas y planes de trabajo del área de informática no se lleva una adecuada administración y control de los equipos de cómputo

6.4.5 RECOMENDACIONES

- ✓ Implementar controles de registro de la recepción y captura de la información.
- ✓ Evaluar la calidad de la captura de los datos.
- ✓ Solicitar inventario de equipo de cómputo al departamento de almacén.
- ✓ Realizar
- ✓ Solicitar por escrito, informar sobre la distribución de equipos de cómputo.
- ✓ Capacitar o recomendar al personal usuario, sobre el adecuado manejo del atasco de papel u objetos extraños en los dispositivos periféricos.

6.5 EVALUACION DE SEGURIDAD

6.5.1 ALCANCE Y OBJETIVOS DE AREA

Integridad de la información almacenada en una computadora.

Integridad, confidencialidad y disponibilidad de los sistemas de información.

Integridad, estabilidad y lealtad del personal.

Operatividad del área de informática.

6.5.2 CUESTIONARIO

Preguntas	SI	NO
1. ¿Conoce las Políticas de Seguridad Informática?		
2. ¿Está el área de informática en un lugar de alto tráfico de personas?		
3. ¿Se tienen materiales o paredes inflamables dentro del área de informática?		
4. ¿Cuenta con aire acondicionado o ventilación?		
5. ¿Existe tierra física y cumple con las especificaciones para los equipos de cómputo?		
6. ¿El cableado se encuentra debidamente instalado e identificado?		
7. ¿Se tienen reguladores para los equipos de cómputo?		
8. ¿Cuenta con medidas de seguridad?		
9. ¿Existe algún tipo de alarmas?		
10. ¿Existen extintores de fuego?		
11. ¿Cuenta con salidas de emergencia?		
12. ¿Existen contraseñas para accesos a los sistemas?		
13. ¿Cuenta con software antiviral original?		
14. ¿Dispone de un programa de copias de respaldo?		
15. ¿Existen medidas de seguridad de los sistemas?		
16. ¿El personal informático está capacitado para aplicar las medidas de seguridad?		

17. ¿Los directivos saben la importancia de las medidas de seguridad?		
18. ¿Existe un plan de contingencias y desastres?		
19. ¿Cuenta con un reglamento interno contra infracciones informáticas?		

6.5.3 HALLAZGOS ENCONTRADOS

- El material de construcción donde está el área informática es altamente inflamable, ya que se encuentra en una cabaña de madera.
- No se cuenta con controles de acceso al área de informática, pero si se ubica en un área de poco tránsito de personas así como de localización a calles de tráfico.
- Si existen extinguidores de fuego así como detectores de humo, pero no se cuenta con aire acondicionado.
- En cuanto a la instalación eléctrica no es adecuada ya que no cuenta con tierra física y esta compartida con una cadena de frío (refrigeradores de biológicos). Se identifica la utilización de multi-contactos y extensiones eléctricas para la conexión de los equipos de cómputo.
- Referente a la seguridad contra virus, en la mayoría de los equipos es inadecuada porque no cuentan con la licencia original del software.
- No se cuenta en jurisdicción con los seguros de la totalidad del equipo de cómputo.
- No existen planes de contingencia y procedimientos de respaldo para casos de desastre.

6.5.4 CONCLUSIONES

La ubicación del área de informática es en una cabaña construida de madera y con paredes que tienen filtraciones de polvo y susceptible a incendio.

Se cuenta con Políticas de Seguridad dadas a conocer por el nivel estatal para el conocimiento y apego del personal a cargo de un equipo de cómputo.

6.5.5 RECOMENDACIONES

- ✓ Aplicar al pie de la letra las Políticas de Seguridad y darlas a conocer al personal de la jurisdicción.
- ✓ Instalar extintores de fuego ya que los cables eléctricos se encuentran expuestos.
- ✓ Colocar señalamiento de salidas de emergencia.
- ✓ Implementar herramientas de seguridad para eliminar las infracciones informáticas.
- ✓ Diseñar un programa de creación de copias respaldo de los sistemas e información.
- ✓ Elaborar un plan de contingencia y procesos de respaldo para casos de desastre.
- ✓ Adquisición de licencias originales para protección de virus.
- ✓ Implementar herramientas de bloqueo para los accesos a internet.
- ✓ Supervisar de forma local los equipos de manejo de los equipos de cómputo de cada departamento.
- ✓ Instalar un sistema no interrumpido (UPS) de batería o de gas, que hace interface entre la energía eléctrica y el dispositivo de entrada de energía a la computadora.

DICTAMEN FINAL

C. Dr. Martin Tejeda Ceballos

Encargado del Despacho de la Jurisdicción Sanitaria, Pátzcuaro

Me dirijo a Ud., con la finalidad de informar que a mi consideración realizar las siguientes recomendaciones, hechas después del análisis realizado en las siguientes fases:

- Función Informática
- Sistemas en desarrollo y en operación
- Procesamiento de datos y equipos de cómputo
- Seguridad

El contenido de este informe ha sido diseñado de la siguiente manera:

- **Situación Actual**, describe las debilidades resultantes del análisis.
- **Efectos y/o implicaciones probables**, describe los posibles riesgos a que se encuentran expuestos las operaciones realizadas por el departamento.
- **Índice de importancia establecida**, indica con una calificación del 0 al 3 el grado crítico del problema y la oportunidad en que se deben tomar las acciones correctivas:

0 = Alto (acciones correctivas inmediatas)

1 = Alto (acciones preventivas inmediatas)

2 = Medio (acciones diferidas correctivas)

3 = Bajo (acciones diferidas preventivas)

- **Sugerencias o alternativas de solución**, describe las propuestas de solución a los puntos críticos.

CARTA DE INTRODUCCIÓN A ALTOS DIRECTIVOS

SITUACIÓN ACTUAL DE LA FUNCION INFORMATICA

- Actualmente el área de informática se encuentra agregada con el departamento de Información en Salud que a su vez dependen del Jefe Jurisdiccional, con funciones de apoyo y soporte para los demás departamentos que cuentan con sistemas de cómputo.
- Se percibe que el área de informática no es de los departamentos estratégicos de alta importancia en la jurisdicción para cumplir con las metas programadas.
- No se ha elaborado programas, planes y procedimientos de trabajo, así como establecer los objetivos y funciones del área de informática.
- El recurso financiero contemplado dentro de los programas de salud, desagregarlo o crear una partida independiente para su adecuada aplicación.

EFFECTOS Y/O IMPLICACIONES PROBABLES

- El no establecer las funciones y objetivos del área de informática no se tendrá un rumbo definido.
- Tomar en consideración el área de informática para la contratación de personal informático.
- Presupuestar recurso financiero para cumplir con las funciones oportunamente.
- El no contar con planes, programas y procedimientos de trabajo, continuara e incluso puede aumentar el despilfarro informático.

ÍNDICE DE IMPORTANCIA ESTABLECIDA

0 = Alto (acciones correctivas inmediatas)

1 = Alto (acciones preventivas inmediatas)

SUGERENCIAS O ALTERNATIVAS DE SOLUCIÓN

- ✓ Es altamente recomendable la descentralización del área de informática como un departamento o coordinación independiente, ya que se obtienen más ventajas sobre la función informática.
- ✓ Otorgar autonomía para toma de decisiones para cumplir con las funciones.
- ✓ Definir las funciones y objetivos del área de informática lo que repercutirá en integración en la toma de decisiones y el logro de las metas de los programas en salud de la jurisdicción.
- ✓ Elaborar programas y procedimientos de trabajo anuales.

SITUACIÓN ACTUAL DE SISTEMAS

- No se desarrollan sistemas y que no se considera la participación del personal, pero si se lleva a cabo la operación de sistemas de información
- Se manejan e instalan software pirata ante la ausencia de un presupuesto de adquisición de permisos o licencias originales.
- Necesidades de desarrollar herramientas o aplicaciones para la automatización de algunos procesos, como por ejemplo; informes mensuales, emisión de oficios de comisión, emisión de cheques, etc.
- Desconocimiento sobre la configuración de los sistemas o programas.
- No se lleva a cabo ningún registro de control sobre incidencias en los sistemas.

EFFECTOS Y/O IMPLICACIONES PROBABLES

- Sistemas de información que no cumplan con todos los requerimientos de los diferentes niveles.
- Mal funcionamiento e inestabilidad o incluso pérdida de la información por uso de software pirata.
- Despilfarro de material de oficina por errores en los reportes.
- Actividades o tareas manuales o mecanizadas.

ÍNDICE DE IMPORTANCIA ESTABLECIDA

0 = Alto (acciones correctivas inmediatas)

1 = Alto (acciones preventivas inmediatas)

SUGERENCIAS O ALTERNATIVAS DE SOLUCIÓN

- ✓ Es de vital importancia disponer de permisos o licencias originales de los sistemas operativos utilizados así como del software ofimática ya que garantiza la funcionalidad de los equipos de cómputo.

U.M.S.N.H.

F.C.C.A. Auditoría Informática en la Jurisdicción Sanitaria Pátzcuaro

- ✓ Para los sistemas de información de uso interno, se propone considerar la participación del área de informática para el desarrollo de sistema a la medida.

SITUACIÓN ACTUAL DEL PROCESO DE DATOS Y EQUIPOS DE CÓMPUTO

- En cuanto al manejo de las bases de datos no se cuenta con controles para el procesamiento de la información.
- No se cuenta con un presupuesto de mantenimiento preventivo y correctivo de los equipos de cómputo, el cual es muy importante para garantizar un óptimo funcionamiento de los equipos.
- No se lleva a cabo ningún registro de control sobre incidencias de los equipos de cómputo.

EFFECTOS Y/O IMPLICACIONES PROBABLES

- Disminuir o eliminar el número de incidencias reportadas para mantenimiento correctivo de los equipos de cómputo.
- Uso de formularios de control de la información capturada ya que garantizara una mejor calidad de los datos procesados.

ÍNDICE DE IMPORTANCIA ESTABLECIDA

0 = Alto (acciones correctivas inmediatas)

1 = Alto (acciones preventivas inmediatas)

SUGERENCIAS O ALTERNATIVAS DE SOLUCIÓN

- ✓ Implementar controles de registro de la recepción y captura de la información.
- ✓ Evaluar la calidad de la captura de los datos.
- ✓ Solicitar inventario de equipo de cómputo al departamento de almacén.
- ✓ Solicitar por escrito, informar sobre la distribución de equipos de cómputo.
- ✓ Capacitar o recomendar al personal usuario, sobre el adecuado manejo de los dispositivos periféricos.

SITUACIÓN ACTUAL DE LA SEGURIDAD

- No cuenta con las instalaciones y medidas de seguridad adecuadas ya que el área de informática se encuentra en el inmueble de un hotel, que actualmente es rentado.
- Cableado eléctrico expuesto a riesgos de cortos circuito, en algunos casos sobrecarga de la línea.
- En cuanto a la seguridad para conexiones en red o internet no se cuenta con herramientas de restricción y control.
- No se cuenta con software antiviral original y no existe un programa de respaldo de información.
- No se cuenta con planes de contingencias y desastres.

EFFECTOS Y/O IMPLICACIONES PROBABLES

- En caso de emergencias no se sabría cómo actuar
- Riesgo a daños funcionales a los equipos de cómputo
- Pérdida total o parcial de la información e inestabilidad de los sistemas
- Contagio y diseminación de virus por toda la red local
- No se sabrá cómo actuar ante un desastre natural o accidental

ÍNDICE DE IMPORTANCIA ESTABLECIDA

0 = Alto (acciones correctivas inmediatas)

1 = Alto (acciones preventivas inmediatas)

SUGERENCIAS O ALTERNATIVAS DE SOLUCIÓN

- ✓ Colocar señalamientos de emergencias
- ✓ Eliminar material inflamable
- ✓ Identificación o señalización adecuada del cableado eléctrico
- ✓ Llevar un estricto control de copias de respaldo de toda la información

U.M.S.N.H.

F.C.C.A. Auditoría Informática en la Jurisdicción Sanitaria Pátzcuaro

- ✓ Adquisición de antivirus original

8. CONCLUSIONES

Durante la investigación identifiqué que el personal directivo del nivel jurisdiccional y estatal, no consideran como indicador importante el administrar las tecnologías de información y comunicación ya que no se aplican controles internos para cumplir con las funciones como departamento de informática.

Otro de los detalles es un rezago considerable la capacitación y la actualización del personal informático de los diferentes departamentos.

El dictamen final propuesto en este trabajo, será considerado, darlo a conocer al responsable estatal del departamento de enlace de informática, para que se tome en consideración para solucionar problemas de funcionamiento del área de informática en las 8 jurisdicciones y 16 hospitales ubicados en el estado.

En la aplicación de los cuestionarios al personal y como resultado de los mismos identifiqué carencias en cuanto a funcionalidad y conocimiento por parte del personal informático y directivo de la jurisdicción, ya que se llegan a tomar malas decisiones en cuanto a la operatividad de los sistemas como del manejo de los equipos de cómputo.

BIBLIOGRAFIA

GARCIA, J. A. (2001). *AUDITORIA INFORMATICA*. MEXICO: MCGRAW-HILL/INTERAMERICANA.

(HERNANDEZ, 2001)

HERNANDEZ, J. R. (2001). *ADMINISTRACION DE LA FUNCION INFORMATICA*. MEXICO: TRILLAS.

ECHENIQUE, JOSE ANTONIO. (2001). *AUDITORIA INFORMATICA*. MEXICO: MCGRAW-HILL.

<http://www.monografias.com/trabajos11/cenco/cenco.shtml>

<http://profesores.fi-b.unam.mx/heriolg/>