UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN - TACNA

ESCUELA DE POSGRADO

MAESTRÍA EN CONTABILIDAD: AUDITORÍA

"EVALUACIÓN DE LOS PROCESOS INFORMÁTICOS A TRAVÉS DE LA AUDITORÍA DE SISTEMAS Y LA EFICIENCIA EN LA GESTIÓN ADMINISTRATIVA DE LA EMPRESA AMERICANA DE DISTRIBUCIÓN Y REPRESENTACIÓN S.A. PERÍODO 2009"

TESIS

Presentado por :

C.P.C. OMAR MARCIAL ESTAÑO MITA

Para Optar el Grado Académico de:

MAESTRO EN CIENCIAS *(MAGISTER SCIENTIAE)*
CON MENCIÓN EN CONTABILIDAD: AUDITORÍA

TACNA - PERÚ
2011

UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN – TACNA

ESCUELA DE POSGRADO

MAESTRÍA EN CONTABILIDAD: AUDITORÍA

"EVALUACIÓN DE LOS PROCESOS INFORMÁTICOS A TRAVÉS DE LA AUDITORÍA DE SISTEMAS Y LA EFICIENCIA EN LA GESTIÓN ADMINISTRATIVA DE LA EMPRESA AMERICANA DE DISTRIBUCIÓN Y REPRESENTACIÓN S.A. PERÍODO 2009"

Tesis sustentada y aprobada el 13 de octubre del 2011; estando el jurado calificador integrado por:

PRESIDENTE : .....
Mgr. Elizabeth Luisa Medina Soto

SECRETARIO : .....
Mgr. Augusto Cahuapaza Morales

MIEMBRO : .....
Mgr. Jorge Gregorio Chambi Velásquez

ASESOR : .....
Mgr. Víctor C. Echegaray Munenaka

DEDICATORIA

A Dios, quien me dio la fortaleza y

la sabiduría para seguir adelante.

A mis Docentes, que me dieron

estímulos de superación.

A mis Padres, por la constante

ayuda para lograr el éxito

académico y profesional.

AGRADECIMIENTOS

Quiero agradecer a todos aquellos que nos apoyaron de manera incondicional, con la única finalidad de lograr el objetivo para obtener el Grado Académico de Maestro con mención en Auditoría.

Primeramente, agradecer a Dios por haberme dado la vida y permitirme conservarla para poder realizar lo que pretendo con el presente trabajo.

Agradecer a mis Padres, quienes me cuidaron y apoyaron desde niño, por haber confiado en mí y haberme brindado el apoyo necesario en la etapa de estudiante, y en mi propia vida.

Agradecer a todas aquellas personas que de diferentes maneras me apoyaron: a los docentes, quienes compartieron sus conocimientos conmigo; a mis amistades, por la fuerza moral y apoyo en los difíciles momentos que lo necesitaba; a todos los seres a los que quiero, por saber comprenderme.

Agradecer a la docente: CPC Elizabeth Medina Soto, por su gran apoyo en el campo de la investigación, y a mi asesor: Doctor Víctor Echegaray Munenaka, quien me acompañó en todo momento, orientándome en el desarrollo y culminación de la tesis.

ÍNDICE GENERAL

Pág.

CAPÍTULO II: MARCO TEÓRICO

CAPÍTULO III: MARCO METODOLÓGICO

RESUMEN

Esta investigación se inserta en el campo de la Auditoría de Sistemas y procura mejoras en la evaluación de los procesos informáticos de la Empresa AMDIRESA S.A.

Diversas investigaciones señalan que los procesos informáticos evalúan los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades del uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse en la gestión administrativa.

Los resultados señalan, al calcular el coeficiente de correlación, la existencia de una relación directa entre las variables, es confiable al realizar el uso del método de consistencia interna Alfa Crombach, obteniéndose el valor de 0,973. El referido valor se considera aceptable estadísticamente por la tendencia de la aproximación a la unidad.

ABSTRACT

This research is inserted in the field of Systems Audit and seeks improvements in the assessment of it processes AMIDRESA Company S.A.

Various research shows that computationally evaluate the documents and records used in preparing the system and all outputs ad reports, the description of the activities of use and its relationship to other systems and files, their frequency of access and conservation, safety and control, the proposed documentation, inputs and outputs of the system and the source documents to be used in administrative management.

The results show, in calculating the correlation coefficient, the existence of a direct relationship between the variables is reliable to make use of the method of internal consistency Cronbach's alpha, yielding the value of 0,973. The aforementioned value is considered statistically acceptable by the tendency of the approximation to the unit.

INTRODUCCIÓN

La presente tesis pretende ser Instrumento Normativo de Gestión Institucional, en el ámbito privado, en el cual se precisan: su naturaleza, la finalidad, funciones generales y funciones específicas en que se describen las atribuciones de las unidades orgánicas y sus relaciones.

Así mismo, se establece una propuesta sobre la "Evaluación de los procesos informáticos a través de la auditoría de sistemas y la eficiencia en la gestión administrativa de la empresa americana de distribuciones y representación S.A., período 2009", especificando su capacidad de decisión, jerarquía del cargo, así como el ámbito de supervisión, adecuándose a los cambios tecnológicos que ocurren en la empresa.

El diseño de la estructura orgánica está orientado al cumplimiento de sus funciones, que permitan lograr las metas, objetivos, asumiendo estrategias propuestas sobre la base del plan maestro optimizado, conllevando a ello a determinar el grado de autoridad y responsabilidad de todos los órganos estructurales, así como los canales de coordinación interna y externa, para coadyuvar con eficiencia y eficacia, orientados a reforzar la prestación de los servicios públicos.

Los avances tecnológicos y la necesidad de tener mejor tiempo y respuesta de la información del sistema, hace que se realicen los distintos

registros de las operaciones, y sirvan de apoyo a la alta dirección en la toma de decisiones.

Se explicará la problemática frente al sistema de información y la toma de decisiones en la empresa AMDIRESA S.A., viendo cómo en la actualidad ésta enfrenta diversos problemas y en qué medida se encuentran afectados, en el manejo efectivo de las informaciones basadas en normas que rigen en nuestro país.

El presente plan de seguridad de la información, del área de tecnología de información de la empresa AMDIRESA S.A., establece el objetivo, alcance y metodología desarrollada en materia de riesgos de tecnología de información. Incluye además, las definiciones utilizadas, las políticas de seguridad del análisis de la situación, el análisis de sensibilidad de la información manejado, la identificación de los riesgos y controles de la tecnología de información (TI).

Permitirá a la auditoría de sistemas, buscar la forma de satisfacer las necesidades, utilizando la información y los recursos de la empresa, creando y brindando los mismos beneficios que se ofrecen en el sistema de información y la toma de decisiones en la empresa AMDIRESA S.A., con la finalidad de obtener en la gestión administrativa un funcionamiento con óptima calidad.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

1.1.1. Antecedentes del problema

El avance científico y tecnológico en la informática viene exigiendo a los empresarios, ejecutivos y profesionales, se capaciten constantemente en los conocimientos de la informática, orientado al movimiento de los procesos informáticos, procesamiento de datos, de las operaciones o actividades; a fin de obtener la rapidez, calidad, oportunidad y confiabilidad en los resultados de la información, para la toma de decisiones de la Alta Dirección.

La empresa AMDIRESA, ha determinado realizar una evaluación de los procesos informáticos, con la finalidad de mejorar la normatividad y teoría que rige en la auditoría de sistemas de esta forma, mejorar la gestión administrativa de la empresa, período 2009.

1.1.2. Problemática de la investigación

En la ciudad de Tacna, en la empresa AMDIRESA, se evidencia que existen deficiencias en la gestión administrativa, debido a que los procesos informáticos no son óptimos, ya que en la organización de los equipos informáticos no se realiza un adecuado mantenimiento correctivo para mejorar en: el funcionamiento del desarrollo de sus programas, documentación de los reportes y de la base de datos; asimismo, el mantenimiento preventivo nos permitirá: la revisión periódica en los equipos informáticos, el desarrollo de sus programas y la base de datos.

Para el control de los procesos informáticos la falta de los sistemas de información van asegurar una mejor: comunicación en los procesos de información, reporte final de los procesos de información, y a realizar los procesos de información en los equipos informáticos.

Al realizar el estudio en la seguridad informática se vio la falta de una seguridad lógica con la finalidad de mejorar: el acceso de seguridad de la base de datos, realizar la verificación de la detección de errores, y la importación y exportación de los datos de información; de tal forma en la

seguridad física se deberá mejorar: El acceso de seguridad, monitoreo y la protección de los equipos informáticos.

En la evaluación tecnológica de los procesos informáticos, la falta de las tecnologías de información, nos permitirá: cumplir con los manuales informáticos, actualizar los nuevos programas y la calidad del servicio en las actividades del proceso de información; la falta de desarrollo con la finalidad de mejorar: el almacenamiento de la información de la base de datos, validación de la información entre el cliente/ servidor y el tiempo de respuesta de información; y la falta de mejorar el soporte técnico con la finalidad de: la protección de la base de datos en la importación de información, utilización de los programas originales y la protección de la base de datos en la exportación de información.

El plan de sistemas de información carece de la elaboración para mejorar en: la documentación, identificación y actualización de la información de la base de datos; así mismo, en la programación para: la compilación de los programas de los procesos de

información, seguridad de los procesos de información a través de la programación, y el uso de los nuevos manuales informáticos.

Ante la propuesta de la auditoría de sistemas, son inadecuadas la evaluación y revisión de los equipos informáticos, de un sistema o procedimiento específico, que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, para lograr el mejoramiento de la gestión en el área de informática.

1.2. Formulación del problema

1.2.1. Pregunta general

¿De qué manera la evaluación de los procesos informáticos, a través de la auditoría de sistemas, influye en la gestión administrativa de la empresa AMDIRESA?, período 2009.

1.2.2. Pregunta específica

a. ¿De qué manera la organización de los equipos informáticos influye en la gestión administrativa de la empresa AMDIRESA?, período 2009.

b. ¿Cómo influye el control de los procesos informáticos en la gestión administrativa de la empresa AMDIRESA?, período 2009.

c. ¿En qué medida influye la seguridad informática en la gestión administrativa de la empresa AMDIRESA?, período 2009.

d. ¿De qué manera incide la evaluación tecnológica de los procesos informáticos en la gestión administrativa de la empresa AMDIRESA?, período 2009.

e. ¿De qué manera incide el plan de sistemas de información en la gestión administrativa de la empresa AMDIRESA?, período 2009.

f. ¿De qué manera influye el manual de la auditoría de sistemas en la gestión administrativa de la empresa AMDIRESA?, período 2009.

1.3. Justificación e Importancia

1.3.1. Justificación

A través de la organización de los equipos informáticos, control de los procesos informáticos, la seguridad

informática, evaluación tecnológica de los procesos informáticos, y el plan de sistemas de información, nos permitirá mejorar el desarrollo de la información por medio una propuesta del desarrollo de un manual de auditoría de sistemas, para que los procesos informáticos distribuyan la información de forma óptima, en la gestión administrativa de la empresa AMDIRESA, durante el período 2009.

1.3.2. Importancia

La adecuada organización de los equipos informáticos, nos permitirá obtener un eficaz funcionamiento (hardware y software) de la información, en la gestión administrativa de la empresa AMDIRESA, período 2009.

Al realizarse el control de los procesos informáticos se observará el dato fuente del movimiento, para la gestión administrativa de la empresa AMDIRESA, período 2009.

Ante el establecimiento de la seguridad informática, se tendrá una protección óptima y cumplimiento de la tecnología de información, en la gestión administrativa de la empresa AMDIRESA, período 2009.

Por medio de la evaluación tecnológica de los procesos informáticos, se tendrá una óptima formación, haciendo el uso de los sistemas de información en la gestión administrativa de la empresa AMDIRESA, período 2009.

A través del plan de sistemas de información, se podrá tener una evaluación tecnológica y el mejoramiento, mediante los cambios del proceso de planificación en la gestión administrativa de la empresa AMDIRESA, período 2009.

Finalmente, el presente estudio propone un manual de auditoría de sistemas, que busca mejorar la distribución de los movimientos de los procesos informáticos en la gestión administrativa de la empresa AMDIRESA, período 2009.

1.4. Alcance y Limitación

1.4.1. Alcance

Los procesos informáticos facilitan a la gestión administrativa, la rapidez del movimiento de la información. Por medio de la auditoría de sistemas los procesos de información serán rápidos y seguros, de forma automatizados.

1.4.2. Limitación

Por medio del avance de la tecnología de la información, se exige a las empresas una ardua capacitación a sus empleados sobre el manejo de los procesos informáticos, para tener una óptima información en la gestión administrativa, dando como resultados la capacidad máxima en los conocimientos de la información.

1.5. Objetivos

1.5.1. Objetivo general

A través de la auditoría de sistemas evaluar si los procesos de informáticos influyen en la gestión administrativa de la empresa AMDIRESA, período 2009.

1.5.2. Objetivo específicos

a. Verificar si la organización de los equipos informáticos, influye en la gestión administrativa de la empresa AMDIRESA, período 2009.

b. Analizar si el control de los procesos informáticos, influye en la gestión administrativa de la empresa AMDIRESA, período 2009.

c. Establecer si la seguridad informática influye en la gestión administrativa de la empresa AMDIRESA, período 2009.

d. Determinar si la evaluación tecnológica de los procesos informáticos, incide en la gestión administrativa de la empresa AMDIRESA, período 2009.

e. Revisar si el plan de sistemas de información, incide en la gestión administrativa de la empresa AMDIRESA, período 2009.

f. Determinar si el manual de auditoría de sistemas, influye en la gestión administrativa de la empresa AMDIRESA, período 2009.

1.6. Hipótesis

1.6.1. Hipótesis general

La evaluación de los procesos de informáticos a través de la auditoría de sistemas, incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

1.6.2. Hipótesis específicas

a. La organización de los equipos informáticos influye significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

b. El control de los procesos informáticos incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

c. La seguridad informática incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

d. La aplicación de una evaluación tecnológica de los procesos informáticos influye significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

e. El plan de sistema de información incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

f. La propuesta de un manual de auditoría de sistemas incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes del estudio

No se ha encontrado trabajos de investigación que se relacionen con algunas de las variables del problema planteado.

Habiéndose revisado en las bibliotecas, hemerotecas de la Universidad Privada de Tacna, y de la Universidad Nacional Jorge Basadre Grohmann de Tacna, no se han encontrado trabajos de investigación, tesis, ni publicaciones realizadas sobre la evaluación en los procesos informáticos y su influencia en la Auditoría de Sistemas, por lo que en esta sección, solamente se hace referencia a obras relacionadas indirectamente a este trabajo de tesis, siendo las siguientes:

Alice Naranjo S. 2010, "Manual de Auditoría de Sistemas", afirma: Mediante el avance de la tecnología de la información (TI), en los equipos informáticos, han ocasionado que en los procesos de información, no sea fácil de entender, manipular y comprender, durante la labor de una Auditoría.

Alice Naranjo S., concluye que: La Informática hoy en día está unida en la gestión de la empresa, y por eso las normas y

estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el (Management) o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoría de sistemas.

Mauricio Solano R. 2008, "Manual de Auditoría de Sistemas", sostiene que: La información y la tecnología que la soporta, representan los activos más valiosos de la empresa, incrementando sus expectativas relacionadas con la entrega de los servicios de Tecnología de Información, la plataforma del usuario, hasta las redes locales o amplias, cliente servidor y equipos Mainframe; por lo tanto, la administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega, al tiempo que demanda que esto se realice a un costo más bajo.

Mauricio Solano R., concluye que: El uso de la informática cubrió las áreas de negocios de todos los niveles con productos y

servicios muy variados. Esta tecnificación del medio imposibilitó al responsable del Área de Informática y a los auditores de sistemas tradicionales seguir evaluando este campo con métodos y procedimientos anticuados. Consecuentemente, se hizo necesario un replanteo del fondo y forma de la auditoría de sistemas.

Enrique Jofré Rojas, 2001 "Modelo de Diseño y Ejecución de Estrategias de Negocios", sostiene que: Los procesos informáticos evalúan los documentos y registros ingresados en el sistema, así como los procedimientos en la comunicación de la información, y el resultado de los reportes almacenados para la seguridad y control de la documentación a usarse.

Enrique Jofré Rojas, concluye que: Ante la inexistencia de información específica, motivo de la presente propuesta, hay dos suposiciones de explicación: Que realmente en los procesos de información y su influencia en el mejoramiento de la gestión de administrativa, es importante para la empresa en su calidad de información y el riesgo a desacreditarse, algunos sectores, tal vez más de lo que ya están, no sacan a luz esta información y le dan un carácter reservado.

EEUU, 2008 "Manual de Función de informática de los Estados Unidos", sostiene que: Los procesos informáticos están dados por

lo siguiente: Que la comunicación entre la información y los equipos informáticos maximizará una óptima calidad a la gestión administrativa de la empresa.

El Manual de Función de informática de los Estados Unidos, concluye que: Asignar los recursos de información a los equipos informáticos, para que la gestión administrativa de la empresa tenga una buena comunicación en la ejecución de la información.

2.2. Bases teóricas

Para fundamentar el problema de la presente investigación que se pretende desarrollar, se hace referencia a las teorías de diversos autores:

Mauricio Solano R., sostiene que: "La función del auditor de sistemas debe ser absolutamente independiente; no tiene carácter ejecutivo ni son vinculantes sus conclusiones. Queda a cargo de la empresa a tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades; estas sugerencias plasmadas en el informe final reciben el nombre de recomendaciones".

Lo importante es lograr mejorar a la entidad, en su control y riesgos. En sí, el auditor de sistemas ayuda a conducir a la entidad en la búsqueda de un desarrollo óptimo en sus procesos informáticos y en todos aquellos elementos que se puedan interrelacionar y aptos en el avance de la Tecnología de la Información.

Miguel H. Bravo Cervantes, sostiene: "Los auditores de sistemas deberán tener conocimientos técnicos necesarios del control, observación y evaluación, para comprender lo que es objeto de su examen, ya que la falta de ellos limita el alcance del trabajo de análisis, aunque procurando no efectuar comentarios definitivos sobre temas que no se hayan podido estudiar, por carecer de dichos conocimientos".

COBIT, sostiene: "Para lograr un eficiente control, se deberá implementar lo necesario dentro de un marco definido para todos los procesos de TI. Ya que los objetivos de control de la tecnología de información están organizados por procesos, se brinda vínculos claros entre los requerimientos de los procesos de TI y los controles de TI."

Es decir, que para enfocarse a una auditoría de sistemas, es importante conocer el control interno y el auditor deberá de trazar

sus metas y objetivos con la finalidad de que su opinión sea concisa.

ISACA, sostiene: "030.010 Código de Ética Profesional.- El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información".

"030.020 Atención profesional correspondiente.- En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional".

INEI, sostiene: "El Auditor de Sistema debe de verificar la existencia y aplicación de todas las normas y procedimientos requeridos para minimizar las posibles causas de riesgos, tanto en las instalaciones y equipos, como en los programas informáticos y los datos, en todo el ámbito del sistema: usuarios, instalaciones, equipos".

La RC – 072 – 98 – CG., establece: "Las normas de control interno que se presentan en esta sección, describen los controles que son necesarios para la implementación en los procesos informáticos de la empresa y el plan de sistemas de información de la entidad, según su actividad y durante un período determinado, así como los

controles de datos fuente, de operación y de salida que preservan el flujo de información, además de su integridad. Asimismo, tales normas desarrollan los controles internos requeridos para el mantenimiento de equipos informáticos y medidas de seguridad para el software (programas informáticos), y hardware (equipamiento informático), así como los aspectos de implementación del Plan de Contingencias de la entidad".

Enrique Jofré Rojas, sostiene que: "Los procesos informáticos evalúan los documentos y registros ingresados en el sistema, así como los procedimientos en la comunicación de la información, y el resultado de los reportes almacenados para la seguridad y control de la documentación a usarse".

Scout George M., sostiene que: "La función básica de los procesos informáticos es garantizar la carga y la ejecución de los procesos, las entradas/salidas y proponer un interfaz entre el proceso de información y la documentación de reportes".

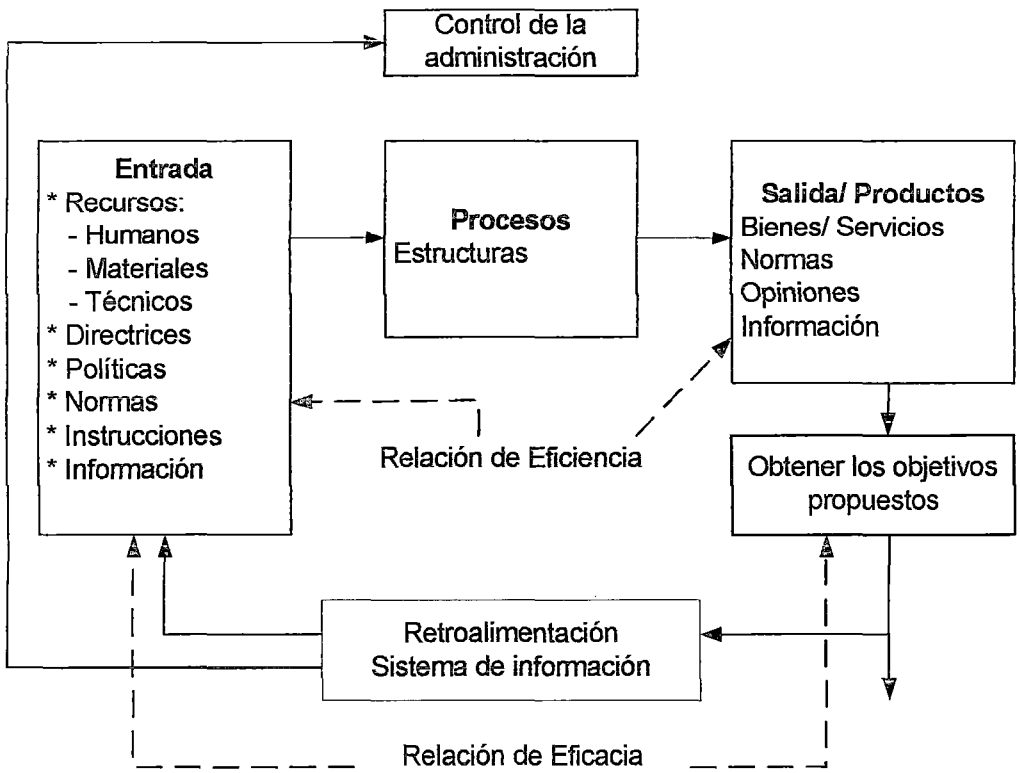
Manual de Función de Informática de EEUU, sostiene que: "El mantenimiento correctivo es la actividad humana desarrollada en los recursos físicos de los equipos informáticos, en consecuencia de una falla han dejado de proporcionar la calidad del servicio del proceso de información".

Manual de Función de Informática de EEUU, sostiene que: "El mantenimiento preventivo es la de inspeccionar los equipos y detectar las fallas en su fase inicial, y corregirlas en el momento oportuno. Se obtiene experiencias en la determinación de causas de las fallas repetitivas o del tiempo de operación seguro de los equipos".

James Martín, sostiene que: "Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo)".

Miguel H. Bravo Cervantes, sostiene que: "Los modernos sistemas de información están cambiando la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos de las empresas, proporcionan información de apoyo al proceso de toma de decisiones y, lo que es más importante, facilitan el logro de ventajas competitivas a través de su implementación en las empresas.

Según Scott, George M., sostiene que: "El Sistema Administrativo lo clasifica por medio de un diagrama"



EL SISTEMA ADMINISTRATIVO

Universidad de Vasco, sostiene que: "La seguridad informática se divide en:

- **Seguridad Lógica:** aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.
- **Seguridad Física:** aplicación de barreras físicas y procedimientos de control, como medidas de prevención y

contramedidas ante amenazas a los recursos e información confidencial".

La Asociación de la Tecnología de Información de América (ITAA), establece que: "Las Tecnologías de Información comprenden todas las tecnologías basadas en los procesos informáticos y comunicaciones a través de los equipos informáticos, usadas para adquirir, almacenar, manipular y transmitir información a los usuarios y unidades de negocios tanto internas como externas".

COSO II, establece que: "Las tecnologías de información reducen ese tiempo y por ende sus costos; esto hace que los administradores y empleados mejoren su productividad, al desperdiciar menos el tiempo en la búsqueda de soluciones a sus problemas".

Juan A. Ferreyros Morón, sostiene que: "La ventana del uso de la tecnología de la información es:

- El uso de las tecnologías de información se ha convertido en un componente central de toda empresa o negocio que busque un crecimiento sostenido.
- Las tecnologías de información pueden significar un incremento en el potencial competitivo de la empresa o

negocio. Actualmente, en la búsqueda de competitividad, se han vuelto los ojos hacia el uso de tecnologías de información".

La Universidad Católica de Chile, establece: "La tecnología puede ser extraordinariamente importante y ayuda a que la Empresa en crecimiento, aumente su comercialización y amplíen sus recursos. La tecnología puede ayudar para poseer infraestructura de almacenamiento de información, permitiéndole aumentar sus ingresos a un ritmo extraordinario".

Julián Gutiérrez Melo, establece que: "El desarrollo de la tecnología de información realiza nuevas aplicaciones de negocios que permitirá proporcionar formas de extraer una ventaja competitiva en el mercado, el uso estratégico de la información aumenta cada vez más en el modelo comercial de éxitos. Crear, compartir y garantizar la seguridad de los datos sea una prioridad principal para el líder del negocio/ tecnología de información en la Empresa de crecimiento".

Ignacio Gil Pechuan, sostiene que: "El ciclo de información de la Empresa es:

- Consolidar el almacenamiento de información.
- Enfrentar problemas de Backup.

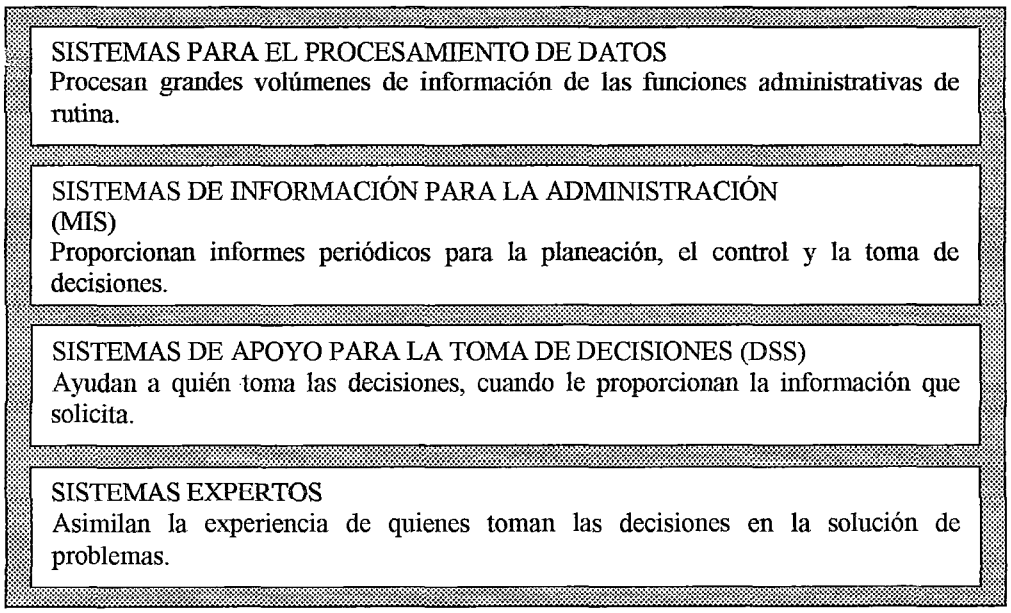
- Construir almacenamiento de información en niveles.
- Optimizar con herramientas de administración".

James A. Senn, establece que: "Las tecnologías de información cambian la manera de realizar las operaciones, que viene haciendo la empresa, ya que la tecnología de información lleva consigo la forma de actuar, por ello deberemos adaptar a los usuarios y la organización a nuevas formas de ejecutar las operaciones, incluyendo estos métodos cuando diseñemos el sistema de información".

Recursos Informáticos de las Entidades del Gobierno Central de Panamá, sostiene que: "Es necesario conocer las tecnologías de información en términos de lo que nos pueden aportar nuevos sistemas de información, pero siempre dentro de la perspectiva del funcionamiento de la Empresa".

Universidad San Martín de Porres, establece que: "La tecnología y las telecomunicaciones cambian día a día, se requiere de mucho tiempo para conocer todos los aspectos tecnológicos que estos cambios suponen y si usted se dedica a conocerlos, no podrá invertir ese tiempo en su propia línea de negocio. Cada actividad profesional requiere de formación continuada".

Miguel H. Bravo Cervantes, el plan de sistema de información para su elaboración lo divide en:



James A. Senn, sostiene que: "La etapa de la programación del plan de sistemas de información se da mediante siete pasos:

- Identificación de problemas, oportunidades y objetivos.
- Determinación de los requerimientos de información.
- Análisis de las necesidades del sistema.
- Diseño del sistema recomendado.
- Desarrollo y documentación del software.
- Prueba y mantenimiento del sistema.
- Implantación y evaluación del sistema".

Kendall Kendall, sostiene que: "El origen de la administración ha existido desde los tiempos más remotos, los relatos Judío/Cristianos de Noe, Abraham y sus descendientes, indican el manejo de gran número de personas y recursos para alcanzar una variedad de objetivos, desde la construcción de alcas, a gobernar ciudades y ganar guerras; muchos textos administrativos citan a Jetro, el suegro de Moisés, como el primer consultor administrativo, él enseñó a Moisés los conceptos de delegación, la administración por excepción y el alcance del control. Las antiguas civilizaciones de Mesopotamia, Grecia y Roma, mostraron los resultados maravillosos de una buena práctica administrativa en la producción de asuntos políticos, el advenimiento de frederick, W. Taylor y la escuela de administración científica, iniciaron el estudio general de administración como disciplina.

Olson, Margrethe H, sostiene que: "Las funciones de la gestión administrativa se clasifican en:

- Planeación.
- Organización.
- Integración de personal.
- Dirección.
- Control".

Agustín Reyes Ponce, sostiene que: "La supervisión de las empresas está en función de una administración efectiva; en gran medida la determinación y la satisfacción de muchos objetivos económicos, sociales y políticos, descansan en la competencia del administrador".

Robert Murdick y Joel Ross, sostiene que: "La planeación es el pensamiento que precede a la acción, comprende el desarrollo de las alternativas y la relación entre ellas, como medida necesaria de acción para lograr un objetivo".

Harold Koontz, prepara a la empresa para hacer frente a las contingencias que se presenten, con las mayores garantías de éxito. Maximiza el aprovechamiento del tiempo y los recursos, en todos los niveles de la empresa.

Robert Murdick y Joel Ross, establece que: "El principio de la planeación se divide en:

- Factibilidad.
- Objetividad y cuantificación.
- Flexibilidad.
- Unidad.
- El cambio de estrategias".

Robert Murdick y Joel Ross, sostiene que: "El control consiste en verificar si todo ocurre de conformidad con el plan adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como fin señalar las debilidades y errores para poder rectificarlos e impedir que se produzcan nuevamente".

Agustín Reyes Ponce, establece que: "La importancia del control se determina y analiza rápidamente las causas que pueden originar desviaciones, para que no se vuelvan a presentar en el futuro".

Agustín Reyes Ponce, sostiene que: "La característica del control es al realizar un buen sistema de control debe manifestar inmediatamente las desviaciones, lo ideal es que las descubra antes de que se produzcan, pues el control será útil en tanto proporcione información en el momento adecuado".

Agustín Reyes Ponce, dice que: "La organización es la estructuración de las relaciones que deben existir entre las funciones, niveles y actividades de los elementos materiales y humanos de un organismo social, con el fin de lograr su máxima eficiencia dentro de los planes y objetivos señalados".

James Martín, sostiene que: "La importancia de la organización es de suministrar los métodos para que se puedan desempeñar las actividades eficientemente, con el mínimo de esfuerzos".

Terry Gorje, sostiene que: "La gestión administrativa está asociada al logro de resultados, por eso es que no debe entenderse como un conjunto de actividades, sino de logros. El proceso de gestión en las instituciones involucra tres aspectos fundamentales como son: el logro de los objetivos, los procesos para alcanzar esos logros, y los recursos utilizados para mejorar la entidad".

2.3. Definición de términos

a. Soporte online

Es un grupo de servicios que proveen asistencia para hardware, software u otros bienes electrónicos o mecánicos. En general, el servicio de soporte técnico sirve para ayudar a resolver los problemas que puedan presentárseles a los usuarios, mientras hacen uso de servicios, programas o dispositivos.

b. Auditoría de software

La auditoría de software consiste en programas informáticos usados por el auditor, como parte de sus procedimientos de auditoría, para procesar datos de importancia de auditoría del sistema de contabilidad de la entidad. Puede consistir en programas de paquete, programas escritos para un propósito, programas de utilería o programas de administración del

sistema. Independientemente de la fuente de los programas, el auditor deberá verificar su validez para fines de auditoría antes de su uso.

c. **Sistema de información**

Es el sistema de personas, registros de datos y actividades, que procesa los datos y la información en cierta organización, incluyendo manuales de procesos o procesos automatizados.

d. **Tecnología de información**

Las tecnologías de Información permiten a la empresa, mejorar su manejo e integración de las necesidades de procesamiento de información, en todas las áreas funcionales de ésta.

e. **La seguridad informática**

La seguridad informática debe formar parte de los lineamientos generales a desarrollarse en base a las directivas emanadas de la gerencia general y formará parte del compromiso de ésta en su aplicación. En ella se deberá establecer con claridad y precisión las metas a alcanzar y las responsabilidades asignadas.

f. **Evaluación de riesgos**

La evaluación de riesgos permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos. La dirección evalúa estos acontecimientos desde una doble perspectiva – probabilidad normalmente, usa una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente y riesgo residual.

g. **Base de datos**

Son programas que administran información y hacen más ordenada la información, aparte de hacerla fácil de buscar. Sus características pueden ser ventajosas o desventajosas: pueden ayudarnos para almacenar, organizar, recuperar, comunicar y manejar información en formas que serían imposibles sin los computadores, pero también nos afecta de alguna manera ya que existen enormes cantidades de información en bases de datos de las que no se tiene control del acceso.

h. **Privacidad de datos**

El grado de avance en estas tecnologías, utilizando sistemas de firewalls físicos y lógicos, como así también, la encripción de datos con un diseño apropiado. Utilizar esta tecnología como la interfase natural de comunicación en todos nuestros sistemas de información, permitiendo que de cualquier parte del mundo se pueda acceder a ellos con la seguridad adecuada.

i. **Firewalls**

Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red de Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

j. **Encripción de datos**

Como sabemos, en un sistema de comunicación de datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma, entre otros aspectos.

k. Virus informáticos

Los virus informáticos son programas que utilizan técnicas sofisticadas, diseñados por expertos programadores, los cuales tienen la capacidad de reproducirse por sí mismos, unirse a otros programas, ejecutando acciones no solicitadas por el usuario, la mayoría de estas acciones son hechas con mala intención.

l. Auditoría informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

m. Auditoría de sistemas

Deberá comprender no sólo la evaluación de los equipos de informáticos, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

n. **Backup**

Es la copia total o parcial de información importante del disco duro, CDs, base de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser: discos duros, CDs, DVDs o cintas magnéticas.

o. **Seguridad lógica**

Se usan para limitar el uso de las aplicaciones de los equipos informáticos, algunos ejemplos son: usuario y contraseña; estos sirven para identificar el usuario y, por lo tanto, con este dato el sistema; otorgará niveles como los siguientes: sólo lectura, lectura modificación, creación, eliminación de registros, ejecutar y copiar. Acceso a los sistemas utilizando tecnologías de información basados en la voz, retina, huella digital. Procedimientos de que consiste en la identificación del usuario a través de su número de línea y luego verificando si este número de línea está autorizado.

p. **Seguridad física**

Corresponde a la Oficina de Informática, en coordinación con la administración de la entidad, establecer los mecanismos de seguridad de los programas y datos del sistema que permitan

asegurar la integridad, exactitud y acceso a las informaciones que se procesan internamente.

q. **Paquete de software**

Los paquetes de software, pueden estar en un formato estandarizado, que le permite ser instalado por un programa que está integrado en el sistema operativo, o puede ser un instalador autosuficiente (no necesita otros programas), generalmente conocido como "instalador".

r. **Sistema operativo**

Es una plataforma para que otros sistemas o aplicaciones la utilicen. Aquellas aplicaciones que permiten ser ejecutadas en múltiples sistemas operativos, son llamadas multiplataforma.

s. **Auditoría de gestión**

Puede definirse como el examen comprensivo y constructivo de la estructura organizativa de una empresa de una institución o departamento gubernamental; o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Tipo y Diseño de la investigación

3.1.1. Tipo de investigación

Por la finalidad que persigue en la mejora de los procesos informáticos a través de la auditoría de sistemas y la eficiencia en la gestión administrativa de la empresa americana de distribuciones y representación S.A., el estudio se identifica como investigación aplicada, de acuerdo a la clasificación que siguen Ander – Egg y Bunge. Este tipo de estudios se caracteriza por la aplicación, utilización y consecuencias prácticas de los conocimientos; es el tipo de investigación que realiza cotidianamente el práctico, el profesional ligado a una institución, empresa u organización. En ese sentido, como señala Ander- Egg, la investigación aplicada busca el conocer para actuar, para construir, para modificar.

Por otro lado, de acuerdo al problema y tipo de conocimiento a lograr, se identifica como investigación de

tipo correlacional. Según Hernández y Col, este tipo de estudios se plantea como una alternativa a los estudios descriptivos y explicativos en tanto va mas allá de la simple descripción de las variables, pero no alcanza el nivel de profundización en la determinación de relaciones causales entre las variables, nivel que caracteriza a los estudios explicativos.

3.1.2. Diseño de la investigación

Para efectos de la contrastación de la hipótesis, se utilizó el diseño no experimental transaccional correlacional, porque procura verificar la existencia de asociación significativa entre las variables. Responde a los diseños no experimentales, porque no recurre a la manipulación de alguna de las variables en estudio, sino que éstas se analizan tal y como suceden en la realidad. Responde a los estudios transaccionales, en tanto la información recogida corresponde a dos períodos; y responde a los estudios correlacionales, porque procura verificar la existencia de asociación significativa entre las variables.

3.2. Población y muestra

La población para el estudio debe estar dada en la organización de los equipos informáticos, control de los procesos informáticos, la seguridad informática, evaluación tecnológica de los procesos informáticos, plan de sistemas de información y la propuesta de la auditoría de sistemas, en la gestión administrativa de la empresa AMDIRESA S.A.; dedicada a la importación de papel Kodak, cámaras fotográficas, y otros útiles de escritorio, cuenta con 23 trabajadores que se encargan de la administración del proceso de información, en cuanto a los aspectos denominados población de objetos y procesos comprenderá las siguientes fuentes de información:

Tabla 01. Población de los funcionarios de la Empresa AMDIRESA

FUNCIONARIOS	N°. DE TRABAJADORES
Junta General de Accionistas	02
Auditoría	02
Directorio	02
Asesoría Legal	01
Gerencia General	01
Departamento de Sistemas	03
Oficina de Administración	02
Departamento de Contabilidad	02
Departamento de Compras	02
Departamento de Almacén zona de Ventas	02
Departamento de Ventas	02
Departamento de Almacén Franco	02
TOTAL	**23**

Debido a que la población mencionada, no tiene un gran tamaño, se ha tomado la decisión de no extraer una muestra, sino que se ha previsto efectuar una encuesta y recolectar la información necesaria de toda la población.

3.3. Operacionalización de variables

3.3.1. Operacionalización de la variable independiente

DETALLE	TIPO VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES
Evaluación de los procesos informáticos a través de la auditoría de sistemas (Variable Independiente)	Cualitativa	Evalúa los documentos y registros usados en la elaboración del sistema, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos y sistemas, su frecuencia de acceso, su conservación, su seguridad y control, la documentación propuesta, las entradas y salidas del sistema y los documentos fuentes a usarse. (Autor: Miguel H. Bravo Cervantes).	Evalúa la eficiencia eficacia, economía de los métodos y procedimientos que rigen el proceso en el Área de informática de la Empresa AMDIRESA.	Organización de los equipos informáticos
				Control de los procesos informáticos
				La seguridad informática
				Evaluación tecnológica de los procesos informáticos.
				Plan de sistemas de información

3.3.2. Operacionalización de la variable dependiente

DETALLE	TIPO VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES
Gestión Administrativa (Variable Dependiente)	Cualitativa	Conjunto de acciones mediante las cuales el directivo desarrolla sus actividades a través del cumplimiento de las fases del proceso administrativo: Planear, organizar, dirigir, coordinar y controlar. (James Martín). Se aplicará mediante el análisis, estudio y evaluación de la información contable, financiera, legal, técnica, administrativa, estadística, propios de los diferentes procesos desarrollados por la entidad en el cumplimiento de su objetivo social; a través de instrumentos de evaluación como: indicadores de gestión, cuadros analíticos, análisis de: la contratación administrativa, recurso humano y financiero, relación beneficio / costo, programas de auditoría, entre otros. (Universidad San Martín de Porres – Lima).	Es el conjunto de decisiones estratégicas mediante las cuales la Empresa AMDIRESA S.A. desarrolla sus actividades a través del cumplimiento de las fases del proceso administrativo: Planear, organizar, dirigir, coordinar y controlar	Planeación
				Control
				Organización

3.4. Técnicas e Instrumentos para recolección de datos

3.4.1. Técnicas de recolección de datos

De acuerdo a la localización de la información, los datos estadísticos pueden ser clasificados en dos tipos: Datos internos de la organización y datos externos.

El método de recopilar datos internos (dentro de la organización) comprenderá la observación directa de la documentación, los procesos y la información pertinente a la investigación.

El método de recopilación de datos externos (fuera de la organización), consistirá en obtener de las publicaciones editadas (por el gobierno, instituciones de investigación, textos, revistas, periódicos, otras ediciones), Internet, doctrinas, manuales, y encuestas (a través de entrevistas y cuestionarios).

3.4.2. Métodos de recolección de datos

Las técnicas e instrumentos que se emplearán para recolectar los datos son:

- **Análisis documental**

  Es una fuente muy valiosa de datos cualitativos, son los documentos, materiales y artefactos diversos. Nos

pueden ayudar a entender el fenómeno central de estudio. Prácticamente la mayoría de las personas, grupos, organizaciones, comunidades y sociedades los producen y narran, o delinean sus historias y estatus actuales. Le sirven al investigador cualitativo para conocer los antecedentes de un ambiente, las experiencias, vivencias o situaciones y su funcionamiento cotidiano.

- **Entrevista**

  En la investigación cualitativa, las primeras entrevistas son abiertas y de tipo "piloto", y van estructurándose conforme avanza el trabajo de campo, pero no es lo usual que sean estructuradas. Debido a ello, el entrevistador o la entrevistadora debe ser altamente calificado en el arte de entrevistar. Coincide en que las entrevistas cualitativas deben ser abiertas, sin categorías, sin categorías preestablecidas, de tal forma que los participantes expresen de la mejor manera sus experiencias y sin ser influidos por la perspectiva del investigador las generan los mismos entrevistados. Al

final cada quien, de acuerdo con las necesidades que plantee el estudio, tomará sus decisiones.

- **Observación global de campo**

  En la investigación cualitativa necesitamos estar entrenados para observar y es diferente de simplemente ver (lo cual hacemos cotidianamente). Es una cuestión de grado. Y la "observación investigativa" no se limita al sentido de la vista, implica todos los sentidos.

- **Cuestionarios**

  Es la técnica de recogida de datos más empleada en investigación, porque es menos costosa, permite llegar a un mayor número de participantes y facilita el análisis, aunque también puede tener otras limitaciones que pueden restar valor a la investigación desarrollada. Estamos hablando muchas veces de escalas de evaluación. Que permiten un escalamiento acumulativo de su ítem, dando puntuaciones globales al final de la evaluación.

3.5. Procesamiento y Análisis de datos

3.5.1. Procesamiento de datos

El procesamiento de datos se hizo de forma automatizada, con la utilización de medios informáticos. Para ello, se utilizaron el soporte informático SPSS 18 Edition, paquete con recursos para el análisis descriptivo de las variables y para el cálculo de medidas inferenciales; y Excel, aplicación de Microsoft Office, que se caracteriza por sus potentes recursos gráficos y funciones específicas que facilitan el ordenamiento de datos. Las acciones específicas en las que se utilizaron los programas mencionados, son las siguientes:

En lo que respecta a Excel:

- Registro de información sobre la base de los formatos aplicados. Este procedimiento permitió configurar la matriz de sistematización de datos, que se adjunta al informe.
- Elaboración de tablas de frecuencia absoluta y porcentual, gracias a que Excel cuenta con funciones para el conteo sistemático de datos, estableciéndose para ello criterios predeterminados.

- Elaboración de los gráficos circulares que acompañan a los cuadros elaborados para describir las variables. Estos gráficos permiten visualizar la distribución de los datos en las categorías que son objeto de análisis. Las tablas y gráficos elaborados con Excel fueron trasladados a Word, para su ordenamiento y presentación final.

En cuanto a SPS 18 Edition:

- Elaboración de las tablas de doble entrada que permite ver el comportamiento conjunto de las variables, según categorías y clases.
- Desarrollo de la prueba chi cuadrado(x^2) y cálculo de la probabilidad asociada a la prueba.

Al igual que con Excel, las tablas y los análisis efectuados fueron trasladados a Word, para su ordenamiento y presentación final.

3.5.2. Análisis de datos

Se utilizaron técnicas y medidas de la estadística descriptiva e inferencial. En cuanto a la Estadística Descriptiva, se utilizaron:

- Tablas de frecuencia absoluta y relativa (porcentual). Estas tablas sirvieron para la presentación de los datos procesados y ordenados según sus categorías, niveles o clases correspondientes.
- Tablas de contingencia. Se utilizó este tipo de tabla para visualizar la distribución de los datos, según las categorías o niveles de los conjuntos de indicadores analizados simultáneamente.

En cuanto a la Estadística Inferencial, se utilizo:

Prueba chi cuadrado (x^2). Esta prueba inferencial, que responde a las pruebas de independencia de criterios, se basa en el principio de que dos variables son independientes entre sí, en el caso que la probabilidad de que la relación sea producto del azar, sea mayor que una probabilidad α fijada de antemano como punto crítico o límite para aceptar la validez de la prueba. En ese sentido, la prueba efectuada y la decisión para la prueba de hipótesis, se basa en el criterio del p- valor. Esto es: si p – valor > α, entonces, las variables son independientes; en otras palabras, no hay relación entre las variables. Por el contrario, si p - valor < α, entonces, para efecto del

estudio, se asume que las variables están relacionadas entre sí. La prueba se ha efectuado mediante lo procedimientos de Pearson y de máxima verosimilitud o razón de verosimilitud. Para la interpretación de resultados, se ha tomado como referencia el valor obtenido por el método de razón de verosimilitud.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Presentación

Este capítulo tiene como finalidad presentar el proceso que conduce a la demostración de la hipótesis propuesta en la investigación, la misma que es la siguiente:

La evaluación de los procesos informáticos a través de la auditoría de sistemas incide significativamente en la gestión administrativa de la empresa AMDIRESA, año 2009.

4.2. Análisis estadístico

4.2.1. Planteamiento del análisis estadístico

a. Antes del tratamiento

Para la recolección de datos, se hizo previamente la validez y la confiabilidad del instrumento.

En el caso de la validez se construyó un instrumento para la realización de la validez de contenido por parte de los expertos. Luego se realizó el análisis de los ítems del cuestionario, haciendo uso del modelo estadístico chi cuadrado(x^2) y, al realizar, una serie

de procesos que implica el método empleado, se llegó a considerar los resultados del anexo Nº. 04 a un nivel de significación del 0,05.

En el caso de la confiabilidad, se usó el método de consistencia interna Alfa Crombach, obteniéndose el valor de 0,973, tal como señala en el anexo Nº 04. El referido valor se considera aceptable estadísticamente por la tendencia de la aproximación a la unidad.

b. **Después del tratamiento**

Se aplicó una encuesta validada, a una población de 23 trabajadores de la empresa AMDIRESA S.A.

A continuación se presenta el análisis de los resultados en las siguientes tablas y gráficos correspondientes.

4.2.2. Resultados

Variable independiente

Indicador: Organización de los equipos informáticos

Tabla 02. Organización de los equipos informáticos

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	17,00	73,98	73,98	73,98
	REGULAR	5,00	21,72	21,72	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

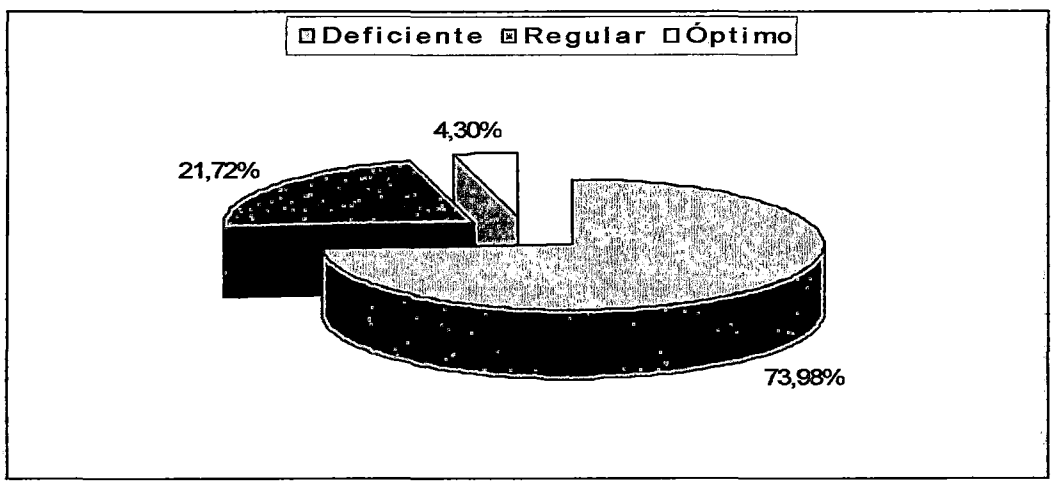


Gráfico 01. Organización de los equipos informáticos

Interpretación

Como se observa en el cuadro, 17 empleados que representan el 73,98% de este conjunto, consideran que la organización de los equipos informáticos de la Empresa AMDIRESA, es deficiente. Asimismo, el 21,72% que constituye 5 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representa el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable independiente

Indicador: Control de los procesos informáticos

Tabla 03. Control de procesos informáticos

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	17,00	73,98	73,98	73,98
	REGULAR	5,00	21,72	21,72	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

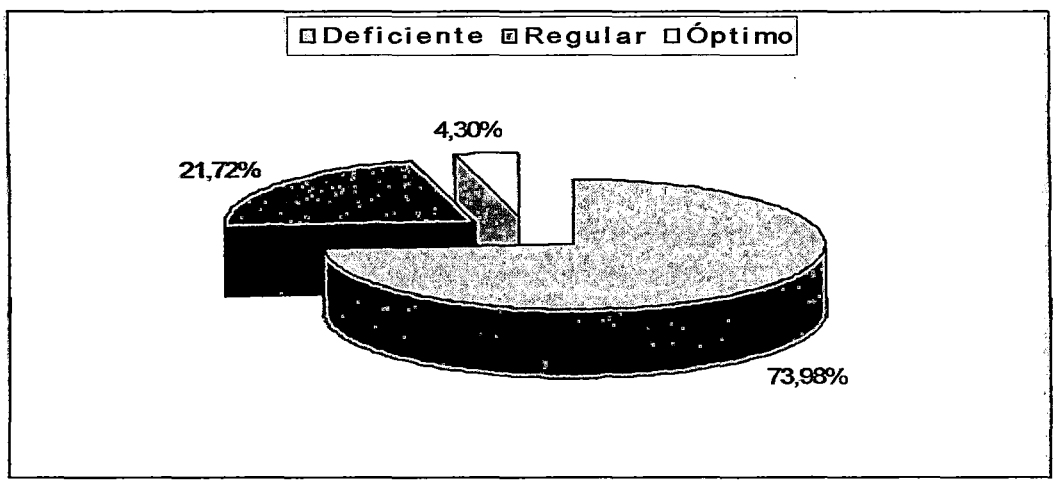


Gráfico 02. Control de procesos informáticos

Interpretación

Como se observa en el cuadro, 17 empleados que representan el 73,98% de este conjunto, consideran que el control de procesos informáticos de la Empresa AMDIRESA, es deficiente. Asimismo, el 21,72% que constituye 5 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representa el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable independiente

Indicador: La seguridad informática

Tabla 04. Seguridad informática

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	18,00	78,30	78,30	78,30
	REGULAR	4,00	17,40	17,40	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

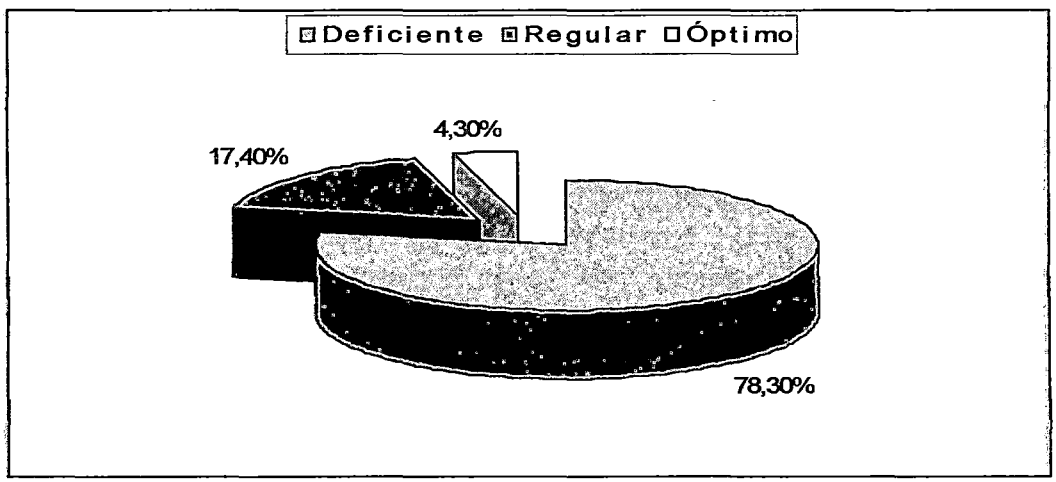


Gráfico 03. La seguridad informática

Interpretación

Como se observa en el cuadro, 18 empleados que representan el 78,30% de este conjunto, consideran que la seguridad informática de la Empresa AMDIRESA, es deficiente. Asimismo, el 17,40% que constituye 4 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representa el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable independiente

Indicador: Evaluación tecnológica de los procesos informáticos

Tabla 05. Evaluación tecnológica de los procesos informáticos

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	18,00	78,30	78,30	78,30
	REGULAR	4,00	17,40	17,40	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

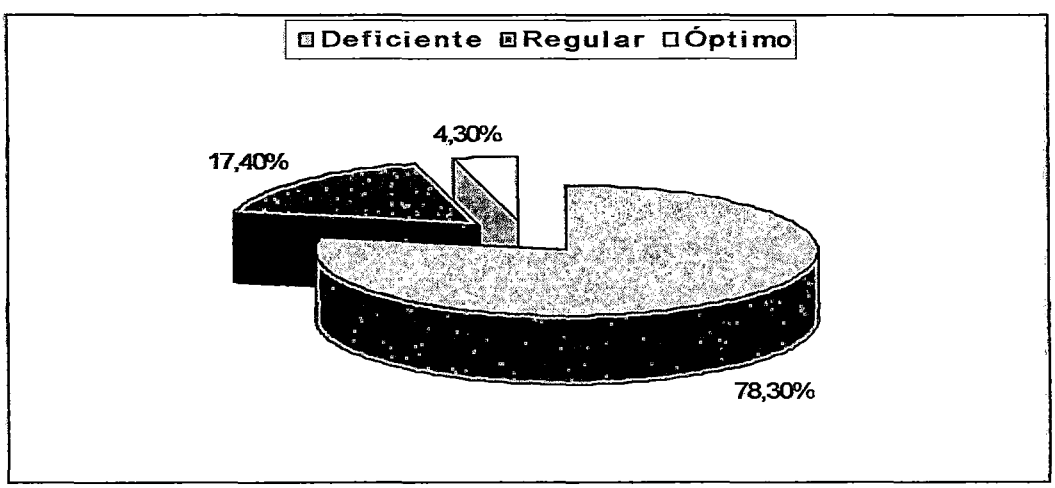


Gráfico 04. Evaluación tecnológica de los procesos informáticos

Interpretación

Como se observa en el cuadro, 18 empleados que representan el 78,30% de este conjunto, consideran que la evaluación tecnológica de los procesos informáticos de la Empresa AMDIRESA, es deficiente. Asimismo, el 17,40% que constituye 4 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representa el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable independiente

Indicador: Plan de sistemas de información

Tabla 06. Plan de sistemas de información

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	17,00	73,98	73,98	73,98
	REGULAR	5,00	21,72	21,72	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

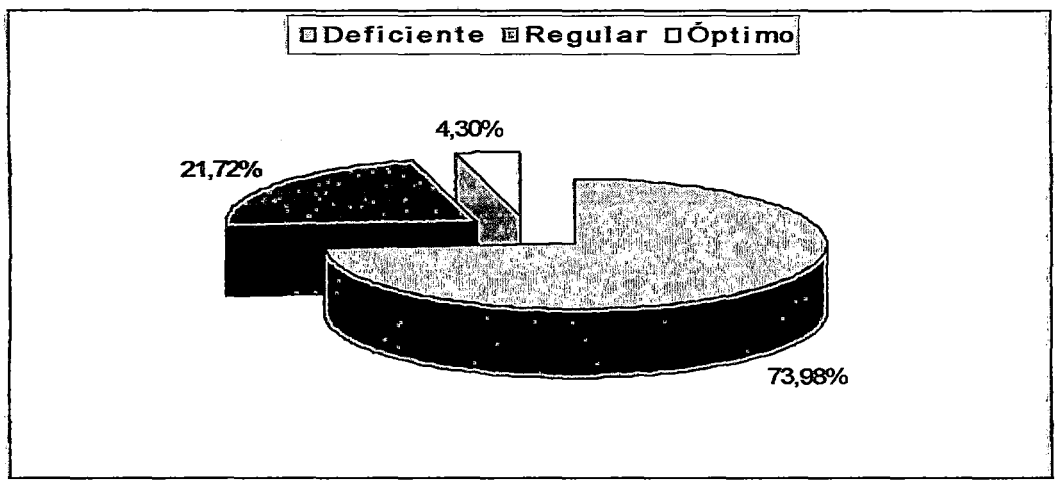


Gráfico 05. Plan de sistemas de información

Interpretación

Como se observa en el cuadro, 17 empleados que representan el 73,98% de este conjunto, consideran que el plan de sistemas de información de la Empresa AMDIRESA, es deficiente. Asimismo, el 21,72% que constituye 5 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representan el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable dependiente

Indicador: Planeación

Tabla 07. Planeación

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	17,00	73,98	73,98	73,98
	REGULAR	5,00	21,72	21,72	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

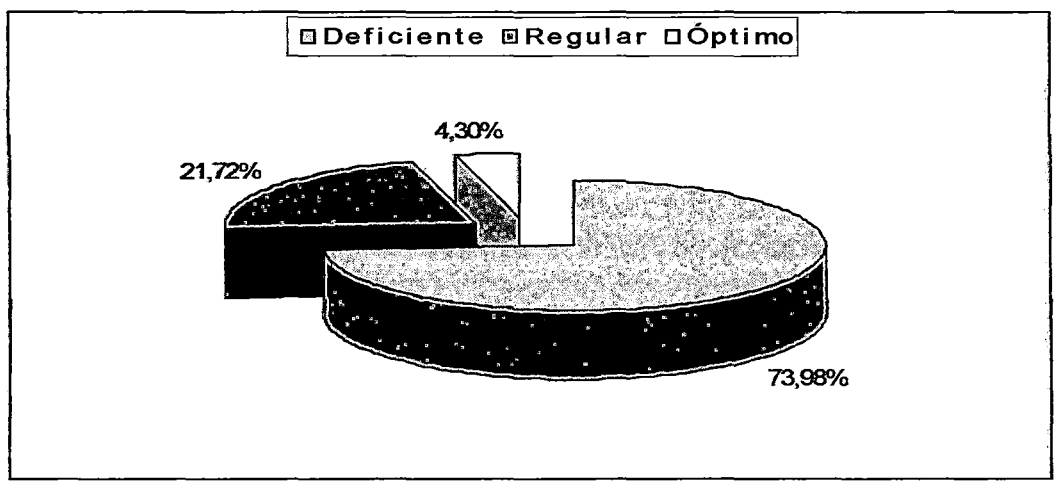


Gráfico 06. Planeación

Interpretación

Como se observa en el cuadro, 17 empleados que representan el 73,98% de este conjunto, consideran que la planeación de la Empresa AMDIRESA, es deficiente. Asimismo, el 21,72% que constituye 5 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representan el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable dependiente

Indicador: Control

Tabla 08. Control

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	17,00	73,98	73,98	73,98
	REGULAR	5,00	21,72	21,72	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

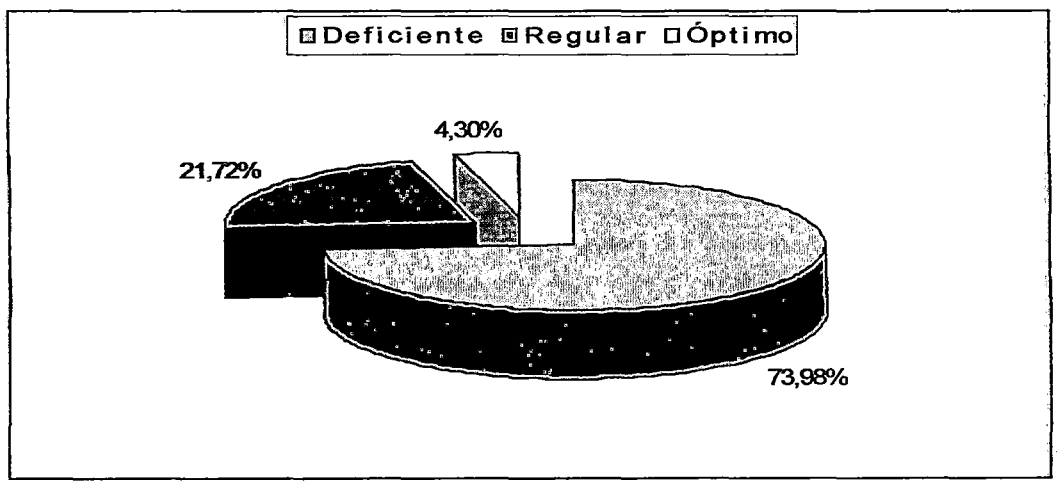


Gráfico 07. Control

Interpretación

Como se observa en el cuadro, 17 empleados que representan el 73,98% de este conjunto, consideran que el control de la Empresa AMDIRESA, es deficiente. Asimismo, el 21,72% que constituye 5 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representa el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

Variable dependiente

Indicador: Organización

Tabla 09. Organización

Descripción		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	DEFICIENTE	17,00	73,98	73,98	73,98
	REGULAR	5,00	21,72	21,72	95,70
	ÓPTIMO	1,00	4,30	4,30	100,00
	Total	23,00	100,00	100,00	

Fuente: Elaboración propia.

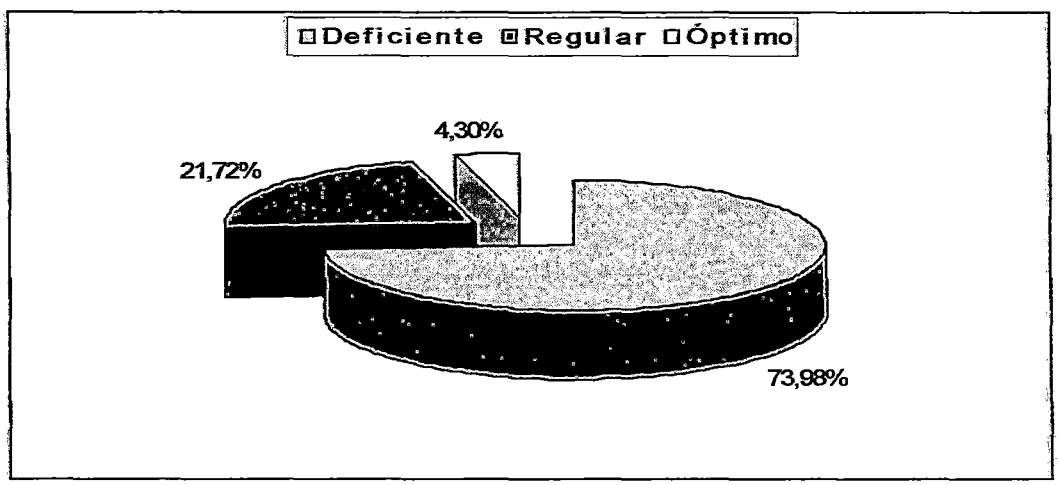


Gráfico 08. Organización

Interpretación

Como se observa en el cuadro, 17 empleados que representan el 73,98% de este conjunto, consideran que la organización de la Empresa AMDIRESA, es deficiente. Asimismo, el 21,72% que constituye 5 empleados, consideran regular el funcionamiento del desarrollo de sus programas; y en contraste, 1 empleado que representa el 4,30%, considera que es óptimo el funcionamiento del desarrollo de sus programas.

4.3. Resultados de la contrastación de la hipótesis

Considerando la hipótesis general y las específicas, planteadas en el trabajo de investigación, con respecto a los procesos informáticos, cuya variable dependiente es la Gestión Administrativa; en donde los ítems, según sus indicadores fueron tabulados con la aplicación del análisis estadístico, en las encuestas efectuadas; se puede afirmar que habrá mayor posibilidad de ser sujeto a la Gestión Administrativa, si no se tiene un óptimo funcionamiento en los procesos informáticos, para fomentar el desarrollo de sus actividades, y lograr la eficiencia, eficacia, economía y efectividad, en las mismas. Si los procesos informáticos no son óptimos, puede ocasionar pérdidas al permitir que la administración utilice información errónea y no pueda tomar decisiones acertadas.

4.3.1. Contrastación de la hipótesis

Tabla 10. Tabla de contingencia Los procesos informáticos a través de la auditoría de sistemas * Gestión Administrativa

Procesos Informáticos		Gestión Administrativa		Total
		deficiente	regular	
Los procesos informáticos a través de la auditoría de sistemas	deficiente	8,00	2,00	10,00
	regular	4,00	4,00	8,00
	eficiente	0,00	5,00	5,00
Total		12,00	11,00	23,00

4.3.2. Pruebas de chi – cuadrado

Tabla 11. Pruebas de chi-cuadrado

Descripción	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	8,573[a]	2,00	0,014
Razón de verosimilitudes	10,743	2,00	0,005
Asociación lineal por lineal	8,008	1,00	0,005
N de casos válidos	23,00		

a. 5 casillas (83,3%) tienen una frecuencia esperada inferior a 5.

La frecuencia mínima esperada es 2,39.

4.3.3. Hipótesis estadística

a. Formulación de hipótesis

Hipótesis nula:

Ho: Los procesos informáticos y la Gestión Administrativa no están relacionadas.

Hipótesis alterna:

H_1: procesos informáticos y la Gestión Administrativa no están relacionados.

b. Nivel de significancia

$\alpha = 0,05$

c. Conclusión

Dado que el pvalor es menor que 0,05; entonces se rechaza la hipótesis nula y se concluye:

"Existe grado de relación entre los procesos informáticos y la Gestión Administrativa".

Es decir, en el siguiente cuadro se observa que hay una tendencia que ilustra, que la tendencia en los procesos informáticos es menor es posible que implique mayor posibilidad de ser sujeto a la Gestión Administrativa. Pero si en los procesos informáticos

es mayor, entonces, es posible que implique menor posibilidad de ser sujeto a la gestión administrativo.

Cabe referir que la variable procesos informáticos y la gestión administrativa, están relacionadas o son dependientes.

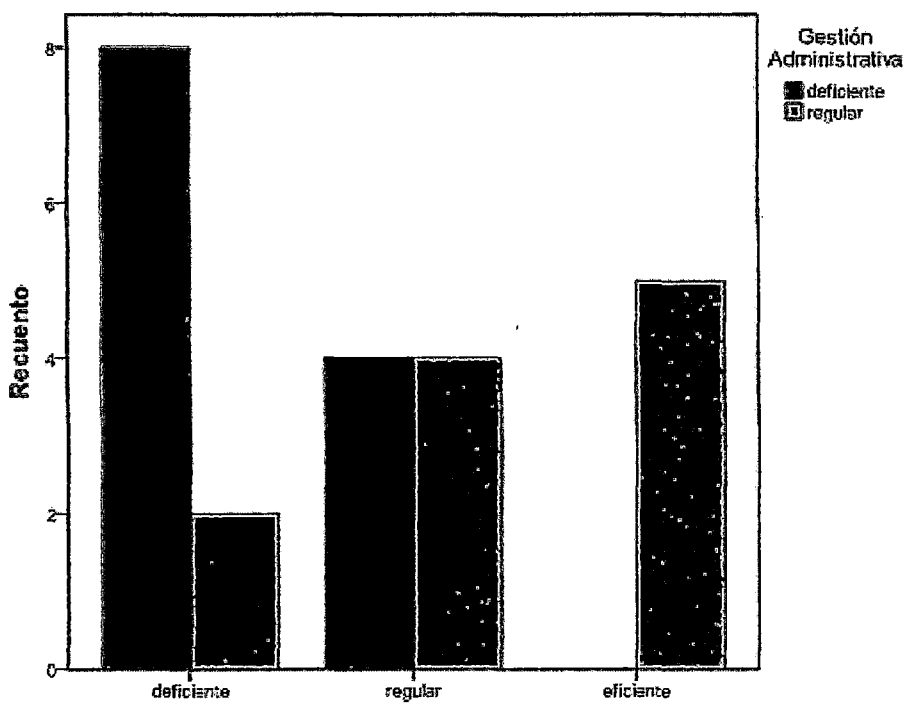


Gráfico 09. Los procesos informáticos a través de la auditoría de sistemas

CAPÍTULO V

PROPUESTA DE UNA AUDITORÍA DE SISTEMAS PARA LA EMPRESA AMDIRESA S.A.

5.1. Teorías existentes sobre auditorías en general

5.1.1. Historia de la auditoría

Existe la evidencia de que alguna especie de auditoría se practicó en tiempos remotos. El hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrolló el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales. La auditoría como profesión, fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general, tuvo lugar durante el período de mandato de la Ley: "Un sistema metódico y normalizado de contabilidad

era deseable para una adecuada información y para la prevención del fraude". También reconocía..."Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas". Desde 1862 hasta 1905, la profesión de la auditoría creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. En Inglaterra se siguió haciendo hincapié en cuanto a la detección del fraude como objetivo primordial de la auditoría. En 1912 Montgomery dijo:

En los que podría llamarse, los días en los que se formó la auditoría, a los estudiantes se les enseñaba que los objetivos primordiales de ésta eran:

- La detección y prevención de fraude.
- La detección y prevención de errores; sin embargo, en los años siguientes hubo un cambio decisivo en la demanda y el servicio, y los propósitos actuales son:
  - El cerciorarse de la condición financiera actual y de las ganancias de una Empresa.
  - La detección y prevención de fraude, siendo éste un objetivo menor.

Este cambio en el objetivo de la auditoría continuó desarrollándose, no sin oposición, hasta aproximadamente 1940. En este tiempo "Existía un cierto grado de acuerdo en que el auditor podía y debería no ocuparse primordialmente de la detección de fraude". El objetivo primordial de una auditoría independiente debe ser la revisión de la posición financiera y de los resultados de operación, como se indica en los estados financieros de los clientes, de manera que pueda ofrecerse una opinión sobre la adecuación de estas presentaciones a las partes interesadas.

Paralelamente, al crecimiento de la auditoría independiente en lo Estados Unidos, se desarrollaba la auditoría interna y del Gobierno, lo que entró a formar parte del campo de la auditoría. A medida que los auditores independientes se apercibieron de la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoría independiente, se mostraron partidarios del crecimiento de los departamentos de auditoría dentro de las organizaciones de los clientes, que se encargaría del desarrollo y mantenimiento de unos

buenos procedimientos del control interno, independientemente del departamento de contabilidad general. Progresivamente, las compañías adoptaron la expansión de las actividades del departamento de auditoría interna hacia áreas que están más allá del alcance de los sistemas contables. En nuestros días, los departamentos de auditoría interna son revisiones de todas las fases de las corporaciones, de las que las operaciones financieras forman parte.

La auditoría gubernamental fue oficialmente reconocida en 1921, cuando el Congreso de los Estados Unidos estableció la Oficina General de Contabilidad.

5.2. Estructura conceptual de la auditoría

La auditoría es el examen de las demostraciones y registros administrativos. El auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos.

Es el examen de todas las anotaciones contables a fin de comprobar su exactitud, así como la veracidad de los estados o situaciones que dichas anotaciones producen.

Es la recopilación de datos sobre información cuantificable de una entidad económica, para determinar e informar sobre el grado de correspondencia entre la información y los criterios establecidos.

Es un proceso a través del cual un sujeto lleva a cabo la revisión de un objeto, con el fin de emitir una opinión acerca de la fidelidad de este (grado de correspondencia), a un patrón o estándar establecido.

Es una función de asesoría técnica al servicio de la Dirección Superior de la Empresa, cuya misión fundamental es apoyar la gestión empresarial, en lo relativo a las necesidades de información, para el proceso de toma de decisiones.

5.3. Objetivo y Fines de la auditoría

5.3.1. Objetivo de la auditoría

El objetivo de la Auditoría consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades. Para ello la Auditoría les proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

5.3.2. Fines de la auditoría

Los fines de la auditoría son los aspectos bajo los cuales su objeto es observado. Podemos escribir los siguientes:

- Indagaciones y determinaciones sobre el estado patrimonial.
- Indagaciones y determinaciones sobre los estados financieros.
- Indagaciones y determinaciones sobre el estado reditual.
- Descubrir errores y fraudes.
- Prevenir los errores y fraudes:
  - Exámenes de aspectos fiscales y legales.
  - Examen para la compra de una empresa (cesión patrimonial).
  - Examen para la determinación de bases de criterios de prorrateo, entre otros.
- Estudios generales sobre casos especiales, tales como:
  - Los variadísimos fines de la auditoría muestran, por sí solos, la utilidad de esta técnica.

5.4. Clases de auditoría

Las clases de auditoría son:

a. **Auditoría externa**

Se puede decir que la auditoría externa es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un Contador Público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento.

El dictamen u opinión independiente tiene trascendencia a los terceros, pues da plena validez a la información generada por el sistema ya que se produce bajo la figura de la Fe Pública, que obliga a los mismos a tener plena credibilidad en la información examinada.

La auditoría externa examina y evalúa cualquiera de los sistemas de información de una organización y emite una opinión independiente, sobre los mismos, pero las empresas generalmente requieren de la evaluación de su sistema de información financiero en forma independiente para otorgarle validez ante los usuarios del producto de éste, por lo cual, tradicionalmente se ha asociado el término auditoría externa a

auditoría de Estados financieros; lo cual como se observa, no es totalmente equivalente, pues puede existir auditoría externa del sistema de información tributario, auditoría externa del sistema de información administrativo, auditoría externa del sistema de información automático y otros.

La auditoría externa o Independiente tiene por objeto averiguar la razonabilidad, integridad y autenticidad de los estados, expedientes y documentos y toda aquella información producida por los sistemas de la organización.

Una auditoría externa se lleva a cabo cuando se tiene la intención de publicar el producto del sistema de información examinado, con el fin de acompañar al mismo una opinión independiente, que le dé autenticidad y permita a los usuarios de dicha información, tomar decisiones confiando en las declaraciones del Auditor.

Una auditoría debe hacerla una persona o firma independiente, de capacidad profesional reconocidas. Esta persona o firma debe ser capaz de ofrecer una opinión imparcial y profesionalmente experta, a cerca de los resultados de auditoría, basándose en el hecho de que su opinión ha de acompañar el informe presentado al término del

examen y concediendo que pueda expresarse una opinión basada en la veracidad de los documentos y de los estados financieros y en que no se imponga restricciones al auditor en su trabajo de investigación.

Bajo cualquier circunstancia, un contador profesional acertado, se distingue por una combinación de un conocimiento completo de los principios y procedimientos contables, juicio certero, estudios profesionales adecuados y una receptividad mental imparcial y razonable.

b. Auditoría interna

La auditoría interna es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la misma. Estos informes son de circulación interna y no tienen trascendencia a los terceros pues no se producen bajo la figura de la fe pública.

Las auditorías Internas son hechas por personal de la empresa. Un auditor interno tiene a su cargo la evaluación permanente del control de las transacciones y operaciones y

se preocupa en sugerir el mejoramiento de los métodos y procedimientos de control interno que redunden en una operación más eficiente y eficaz. Cuando la auditoría está dirigida por contadores públicos profesionales independientes, la opinión de un experto desinteresado e imparcial constituye una ventaja definida para la empresa y una garantía de protección para los intereses de los accionistas, los acreedores y el público. La imparcialidad e independencia absolutas no son posibles en el caso del auditor interno, puesto que no puede divorciarse completamente de la influencia de la alta administración, y aunque mantenga una actitud independiente como debe ser, ésta puede ser cuestionada ante los ojos de los terceros. Por esto se puede afirmar que el auditor no solamente debe ser independiente, sino parecerlo para así obtener la confianza del público.

La auditoría interna es un servicio que reporta al más alto nivel de la dirección de la organización y tiene características de función asesora de control, por tanto no puede ni debe tener autoridad de línea sobre ningún funcionario de la empresa, a excepción de los que forman parte de la planta de la oficina de auditoría interna, ni debe en modo alguno

involucrarse o comprometerse con las operaciones de los sistemas de la empresa, pues su función es evaluar y opinar sobre los mismos, para que la alta dirección toma las medidas necesarias para su mejor funcionamiento.

La auditoría Interna sólo interviene en las operaciones y decisiones propias de su oficina, pero nunca en las operaciones y decisiones de la organización a la cual presta sus servicios, pues como se dijo es una función asesora.

5.5. Diferencia entre auditoría interna y auditoría externa

Auditoría interna	Auditoría externa
Existe un vínculo laboral entre el auditor y la empresa.	La relación es de tipo civil.
El diagnóstico del auditor, está destinado para la empresa.	Este dictamen se destina generalmente para terceras personas, o sea, ajena a la empresa.
Está inhabilitada para dar Fe Pública, debido a su vinculación contractual laboral.	Tiene la facultad legal de dar fe pública.

5.6. Funciones de la auditoría

- Experiencia en el campo de La contabilidad.
- Destreza en el manejo de métodos de recolección de datos e información.
- Responsabilidad sobre un dictamen profesional ante terceras personas.

5.7. Función del auditor

Es emitir dictámenes independientes, y calificados acerca de informes administrativos, con base en un análisis de la información objetiva subyacente a los datos suministrados y estudiados.

5.8. Tipos de auditoría

a. Auditoría financiera

Consiste en una revisión exploratoria y crítica de los controles subyacentes y los registros de contabilidad de una empresa, realizada por un contador público, cuya conclusión es un dictamen a cerca de la corrección de los estados financieros de la empresa.

b. Auditoría operativa

Se define como una técnica para evaluar sistemáticamente de una función o una unidad conferencia a normas de la empresa, utilizando personal no especializado en el área de

estudio, con el objeto de asegurar a la administración, que sus objetivos se cumplan, y determinar que condiciones pueden mejorarse.

c. **Auditoría de sistemas**

Es la verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.

d. **Auditoría gubernamental**

Revisión y examen que llevan a cabo la Secretaría de Contraloría y Desarrollo Administrativo y/o la Entidad de Fiscalización Superior de la Federación, a las operaciones de diferente naturaleza, que realizan las dependencias y entidades del Gobierno Federal, Estatal y Municipal, en el cumplimiento de sus atribuciones.

5.9. El control interno de las entidades a auditarse

5.9.1. Antecedentes

El origen del control interno, suele ubicarse en el tiempo con el surgimiento de la partida doble, que fue una de las medidas de control, pero no fue hasta fines del siglo XIX que los hombres de negocios se preocuparon por formar y

establecer sistemas adecuados para la protección de sus intereses.

A finales de este siglo, como consecuencia del notable aumento de la producción, los propietarios de los negocios se vieron imposibilitados de continuar atendiendo personalmente los problemas productivos, comerciales y administrativos, viéndose forzados a delegar funciones dentro de la organización conjuntamente con la creación de sistemas y procedimientos que previeran o disminuyeran fraudes o errores, debido a esto comenzó a hacerse sentir la necesidad de llevar a cabo un control sobre la gestión de los negocios, ya que se había prestado más atención a la fase de producción y comercialización, que a la fase administrativa u organizativa, reconociéndose la necesidad de crear e implementar sistemas de control, como consecuencia del importante crecimiento operado dentro de las entidades.

Se puede afirmar que el control interno ha sido preocupación de la mayoría de las entidades, aunque con diferentes enfoques y terminologías, lo cual se puede evidenciar al consultar los libros de texto de auditoría, los

artículos publicados por organizaciones profesionales, universidades y autores individuales.

5.10. Definición del control

El sistema de control interno comprende el plan de la organización y todos los métodos coordinados y medidas adoptadas dentro de una empresa, con el fin de salvaguardar sus activos y verificara la confiabilidad de los datos contables.

El sistema de control interno de una empresa forma parte del control de gestión de tipo táctico y está constituido por el plan de organización, la asignación de deberes y responsabilidades, el sistema de información financiero y todas las medidas y métodos encaminados a proteger los activos, promover la eficiencia, obtener información financiera confiable, segura y oportuna y lograr la comunicación de políticas administrativas y estimular y evaluar el cumplimientos de éstas últimas.

5.11. Importancia del control interno

El control interno contribuye a la seguridad del sistema contable que se utiliza en la empresa, fijando y evaluando los procedimientos administrativos, contables y financieros, que ayudan a que la empresa realice su objeto. Detecta las irregularidades y errores y propugna por la solución factible,

evaluando todos los niveles de autoridad, la administración del personal, los métodos y sistemas contables, para que así el auditor pueda dar cuenta veraz de las transacciones y manejos empresariales.

5.12. Clasificación del control interno

En un sentido amplio el control interno incluye controles que pueden ser catalogados como contables o administrativos.

La clasificación entre controles contables y controles administrativos, variaría de acuerdo con las circunstancias individuales.

a. Control administrativo

Los controles administrativos comprenden el plan de organización y todos los métodos y procedimientos relacionados principalmente con eficiencia en operaciones y adhesión a las políticas de la empresa y, por lo general, solamente tienen relación indirecta con los registros financieros. Incluyen más que todo, controles tales como: análisis estadísticos, estudios de moción y tiempo, reportes de operaciones, programas de entrenamientos de personal y controles de calidad.

En el Control Administrativo se involucran: el plan de organización y los procedimientos y registros relativos a los procedimientos decisorios, que orientan la autorización de transacciones por parte de la gerencia. Implica todas aquellas medidas relacionadas con la eficiencia operacional y la observación de políticas establecidas en todas las áreas de la organización.

Estos controles administrativos interesan en segundo plano a los Auditores independientes, pero nada les prohíbe realizar una evaluación de los mismos hasta donde consideren sea necesario para lograr una mejor opinión.

El control administrativo se establece en el SAS-1 de la siguiente manera:

El control administrativo incluye, pero no se limita al plan de organización, procedimientos y registros que se relacionan con los procesos de decisión que conducen a la autorización de operaciones por la administración. Esta autorización es una función de la administración asociada directamente con la responsabilidad de lograr los objetivos de la organización y es el punto de partida para establecer el control contable de las operaciones. [SAS.1].

b. **Control contable**

Los controles contables comprenden el plan de organización y todos los métodos y procedimientos relacionados principal y directamente a la salvaguardia de los activos de la empresa y a la confiabilidad de los registros financieros. Generalmente incluyen controles, tales como: el sistema de autorizaciones y aprobaciones con registros y reportes contables de los deberes de operación y custodia de activos y auditoría interna.

5.13. Componentes del control interno

Dentro del marco integrado se identifican cinco elementos de control interno que se relacionan entre sí y son inherentes al estilo de gestión de la empresa. Los mismos son:

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Supervisión o monitoreo.

5.14. Diseñando un sistema de control interno

5.14.1. Diseño del sistema

Consiste en:

- Armar el flujo de información.
- Diseñar los sistemas de control de custodia.
- Debemos puntualizar cómo se realizan los intercambios en el ente.
- El armado del sistema de control debe contener:
  - Los medios de información (listado de computador, y otros).
  - Los comprobantes y medios magnéticos de tratamiento y traslado de información.
  - Los procesos manuales y computarizados que se utilizan.
  - Los procedimientos establecidos para que la operatoria funcione organizadamente.
  - Los departamentos involucrados.
  - Las personas involucradas.
  - Los asientos para retención de datos.

5.14.2. Los procesos de creación de los controles

Tenemos que contemplar los aspectos relevantes para poder diseñar un sistema de control interno que consiste en los siguientes pasos:

- Identificar los departamentos involucrados y relacionarlos con documentos o medios magnéticos.
- Analizar la segregación de funciones.
- Identificar los puntos débiles de control.
- Para cada punto de control, detallar la totalidad de los errores posibles.
- Para cada uno de los posibles errores arriba identificados, establecer un método de control.
- Para los métodos de control establecidos, analizar su costo beneficio.
- Para los métodos de control establecidos, analizar la segregación de funciones.

5.14.3. Análisis de proceso

a. Identificar los departamentos involucrados y relacionarlos con documentos o medios magnéticos

Cuando se diseña el flujo de información, se establece los medios en los cuales dicha información se almacena. Estos medios de información pueden ser magnéticos o medios manuales. Debemos entonces identificar los departamentos involucrados.

b. **Analizar la segregación de funciones**

La identificación expuesta se realiza con el objetivo de analizar la segregación, las funciones como un prerrequisito de control. Si no existe una adecuada segregación de funciones a nivel de la arquitectura del sistema, el mismo se caracteriza por su falibilidad, es decir, la posibilidad de que sea violado.

La segregación de funciones reviste fundamental importancia, tanto para el auditor, como para aquel que diseña el sistema, en la medida que el arquitecto quiera asegurar la relativa seguridad.

c. **Identificar los puntos de control**

Debemos separar el procesamiento de la información en tres categorías:

- **Procesamiento de la información**

  En el procesamiento se puede dar los errores establecidos y habrá que identificar dónde se pueden producir esos errores de población y exactitud.

- **Captura de la información**

  Es la información que se captura dentro del proceso de información.

- **Custodia de los bienes**

  Aplican los mismos criterios expuestos para el punto anterior.

d. **Para cada uno de los posibles errores arriba identificados, establecer un método de control**

   Se debe diseñar los controles que prevengan o detecten los posibles errores identificados el punto anterior.

e. **Para los métodos de control establecidos, analizar su costo beneficio**

   El costo del control no puede ser mayor al valor que se controla. Pero es dificultoso determinar dicho valor. Este aspecto debe ser analizado para cada sistema y control en particular y depende de las características y valores organizacionales de cada empresa.

f. **Para los métodos de control establecidos, analizar la segregación de funciones**

Una vez establecidos los métodos de control, lo que debemos analizar es si las personas involucradas en el proceso de control cumplen con los requisitos de separación de funciones. Aquí nos interesamos:

- Que el control se dé por oposición de intereses entre las partes a cargo de la operación
- Que los que tienen funciones exclusivas de control no estén involucrados en tareas operativas, en relación con el sistema que se está diseñando.

5.15. Implantación del sistema de control interno

La principal función de este servicio es brindar una eficiencia operativa de la Empresa, basándose en el estudio y evaluación de la misma, dando cumplimiento a los objetivos de control interno.

Les proporcionamos a nuestros clientes los elementos necesarios para crear un ambiente de control óptimo, para cumplir con los siguientes objetivos de control interno:

- Salvaguarda de los activos de la entidad.
- Apego a las políticas establecidas por la administración de la compañía.

- Obtención de información oportuna, veraz y confiable.

El servicio consta principalmente de implantar el control interno en la Empresa, dando como resultado el establecimiento de un manual de políticas y procedimientos, así como la capacitación al personal que intervendrá directamente en su aplicación.

5.16. Normas de control interno para los sistemas informáticos

5.16.1. El jefe de informática

Debe ejercer un papel muy importante como transmisor de información entre el departamento de informática y la organización. Es el puente de comunicación en ambas direcciones (técnicamente hablando).

Esto quiere decir que el jefe de informática posee información relativa a la situación de la organización que el personal técnico no es necesario que conozca. Además, el jefe se ocupa de velar por una serie de proyectos que desempeñan los administradores (o incluso otros departamentos o aquellos que se encuentran contratados externamente), relativos a la informática de la organización.

Tal y como se ven en el gráfico anterior, la figura del jefe de informática es la que gestiona los recursos del departamento (tanto humanos, como materiales). Por lo

tanto, debe tener un conocimiento perfecto de la organización y del departamento, para conseguir que los dos elementos se desarrollen lo más sincronizadamente posible. Debe lograr que el departamento de informática se ajuste perfectamente a los objetivos de la organización con los recursos que ésta última le facilite. En la práctica, actúa siempre como un canal de comunicación, en ambos sentidos, para detectar necesidades, obtener recursos, ajustar objetivos, y otros.

El jefe de informática gestiona los recursos del departamento de informática y actúa de enlace entre el Departamento y la Organización.

5.16.2. El papel del auditor de sistemas

Comprende las tareas de evaluar, analizar los procesos informáticos, el papel de auditor debe estar encaminado hacia la búsqueda de problemas existentes dentro de los sistemas utilizados y, a la vez, proponer soluciones para estos problemas.

El Auditor de Sistemas debe estar capacitado en los siguientes aspectos:

a. Deberá ver cuándo se puede conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada, estando obligado a presentar recomendaciones acerca del reforzamiento del sistema y del estudio de las soluciones más idóneas, según los problemas detectados en el sistema informático, siempre y cuando las soluciones que se adopten no violen la ley ni los principios éticos. (Ej. Por qué está mal el reporte).

b. Una vez estudiado el sistema informático a auditar, el auditor deberá establecer los requisitos mínimos, aconsejables y óptimos para su adecuación con la finalidad de que cumpla para lo que fue diseñado, determinando en cada clase su adaptabilidad, su fiabilidad, limitaciones, posibles mejoras, costos.

c. Lógicamente el auditor deberá abstenerse de recomendar actuaciones innecesariamente onerosas, dañinas, o que generen riesgo injustificativo para el auditado e igualmente de proponer modificaciones carentes de bases

científicas insuficientemente probadas o de imprevisible futuro.

d. El auditor, al igual que otros profesionales (Ej. Médicos, abogados, educadores, etc.) pueden incidir en la toma de decisiones en la mayoría de sus clientes con un elevado grado de autonomía, dado la dificultad práctica de los mismos, de constatar su capacidad profesional y en desequilibrio de desconocimientos técnicos existentes entre al auditor y los auditados (Puede pesar gravemente).

e. El auditor deberá prestar sus servicios de acuerdo a las posibilidades de la ciencia y a los medios a su alcance con absoluta libertad, respecto a la utilización de dichos medios y en unas condiciones técnicas adecuadas para el idóneo cumplimiento de su labor. En los casos en que la precariedad de los medios puestos a su disposición, impidan o dificulten seriamente la realización de la auditoría, deberá negarse a realizar esta tarea, hasta que se le garantice un mínimo de condiciones técnicas que no

comprometan la calidad de sus servicios o dictámenes.

f. Cuando durante la ejecución de la auditoría, el auditor considere conveniente recabar informe de otros más calificados, sobre un aspecto o incidencia que superase su capacidad profesional para analizarlo en idóneas condiciones, deberá remitir el mismo a un especialista en la materia o recabar su dictamen para reforzar la calidad y viabilidad global de la auditoría.

g. El auditor debe actuar con cierto grado de humildad evitando dar la impresión de estar al corriente de una información privilegiada sobre nuevas tecnologías a fin de actuar en previsiones rectas y un porcentaje de riesgo debidamente fundamentado.

h. El auditor, tanto en sus relaciones con el auditado como con terceras personas, deberá actuar en todo momento, conforme a las normas implícitas o explícitas de dignidad de la profesión y de corrección en el trato personal.

i. El auditor deberá facilitar e incrementar la confianza del auditado en base a una actuación de transparencia en su actividad profesional, sin alardes científico técnicos, que, por su incomprensión, pueden restar credibilidad a los resultados obtenidos y a las directrices aconsejadas.

5.17. El jefe de informática y el administrador de sistemas

Tiene una visión más global de todo. Por lo tanto, necesita la figura del administrador, que es quien cuida de los servidores. El administrador le indica la situación y la visión técnica del departamento de informática en cada momento. Por lo tanto, le puede asesorar para tomar muchas decisiones sobre software y hardware. En la práctica, la mayoría de decisiones técnicas se toman con la ayuda del administrador de sistemas.

5.18. Los planes

Todas las organizaciones, con el fin de estar coordinadas y preparadas para cualquier situación, siguen una serie de planes que los jefes de cada departamento deben preparar, revisar y tener a punto.

5.19. Plan de contingencias

El plan de contingencias, aplicado sólo al entorno informático, es un plan que implica analizar los posibles riesgos a los que puede estar expuesto el equipamiento informático y la información que poseemos (en cualquier medio de almacenamiento). El objetivo es doble. Por una parte, reducir la posibilidad de que pueda ocurrir algún percance y, por otra, si ocurre, prever las acciones y actuaciones que son precisas poner en práctica en estas situaciones.

Debido al riesgo de que a pesar de todas las medidas que se tomen puede ocurrir un percance, el plan de contingencia incluye un plan de recuperación de desastres, que tiene el objetivo de restaurar el servicio informático cuanto antes y minimizar el coste y las pérdidas en la medida en que se pueda.

Para que el diseño del plan de contingencias tenga sentido, se debe presuponer el peor caso de todos, el desastre total. De esta manera, el plan será lo más completo posible y podrá incluir toda la casuística.

5.20. El análisis de riesgos

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la

seguridad física, que se establezca sobre los equipos en los cuales se almacena. Estas técnicas brindan la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: "lo que no está permitido debe estar prohibido" y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas informáticos.

5.21. Elementos del análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático, se pueden tomar los siguientes puntos como referencia a seguir:

a. Construir un perfil de las amenazas que esté basado en los activos de la organización.
b. Identificación de los activos de la organización.
c. Identificar las amenazas de cada uno de los activos listados.
d. Conocer las prácticas actuales de seguridad.
e. Identificar las vulnerabilidades de la organización.
    - Recursos humanos
    - Recursos técnicos
    - Recursos financieros
f. Identificar los requerimientos de seguridad de la organización.

g. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.

h. Detección de los componentes claves.

i. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

- Riesgo para los activos críticos,
- Medidas de riesgos,
- Estrategias de protección,
- Planes para reducir los riesgos.

5.22. Análisis del impacto de negocio

El reto es asignar estratégicamente los recursos para el equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los Valores para el sistema, se pueden distinguir: Confidencialidad de la información, la Integridad

(aplicaciones e información) y finalmente, la disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor Web público puede poseer los requisitos de confidencialidad de baja (ya que toda la información es pública). En contraste, un sistema de planificación de recursos empresariales (ERP), poseer alto puntaje en las tres variables. Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

5.23. Puesta en marcha de una política de seguridad

Actualmente, las legislaciones nacionales de los Estados, obligan a las empresas a implantar una política de seguridad.

Generalmente, se ocupa exclusivamente de asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso, en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización,

- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión,
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

5.24. Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguros, todavía deben ser tenidas en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única

protección posible es la redundancia (en el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta a intrusos o bien, modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
- Un intruso: persona que consigue acceder a los datos o programas a los cuales no tiene acceso permitido.
- Un siniestro (robo, incendio, inundación): una mala manipulación o una mal intención, derivan en la pérdida del material o de los archivos.
- El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

5.25. Técnicas para asegurar el sistema

a. Consideraciones de software

Tener instalado en la máquina únicamente el software necesario, reduce riesgos. Así mismo, tener controlado el software, asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías, aumenta los riesgos). En todo caso, un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos, facilita también la reinstalación en caso de contingencia.

Existe un software que es conocido por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades, pero permitiendo una seguridad extra.

b. Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas Web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

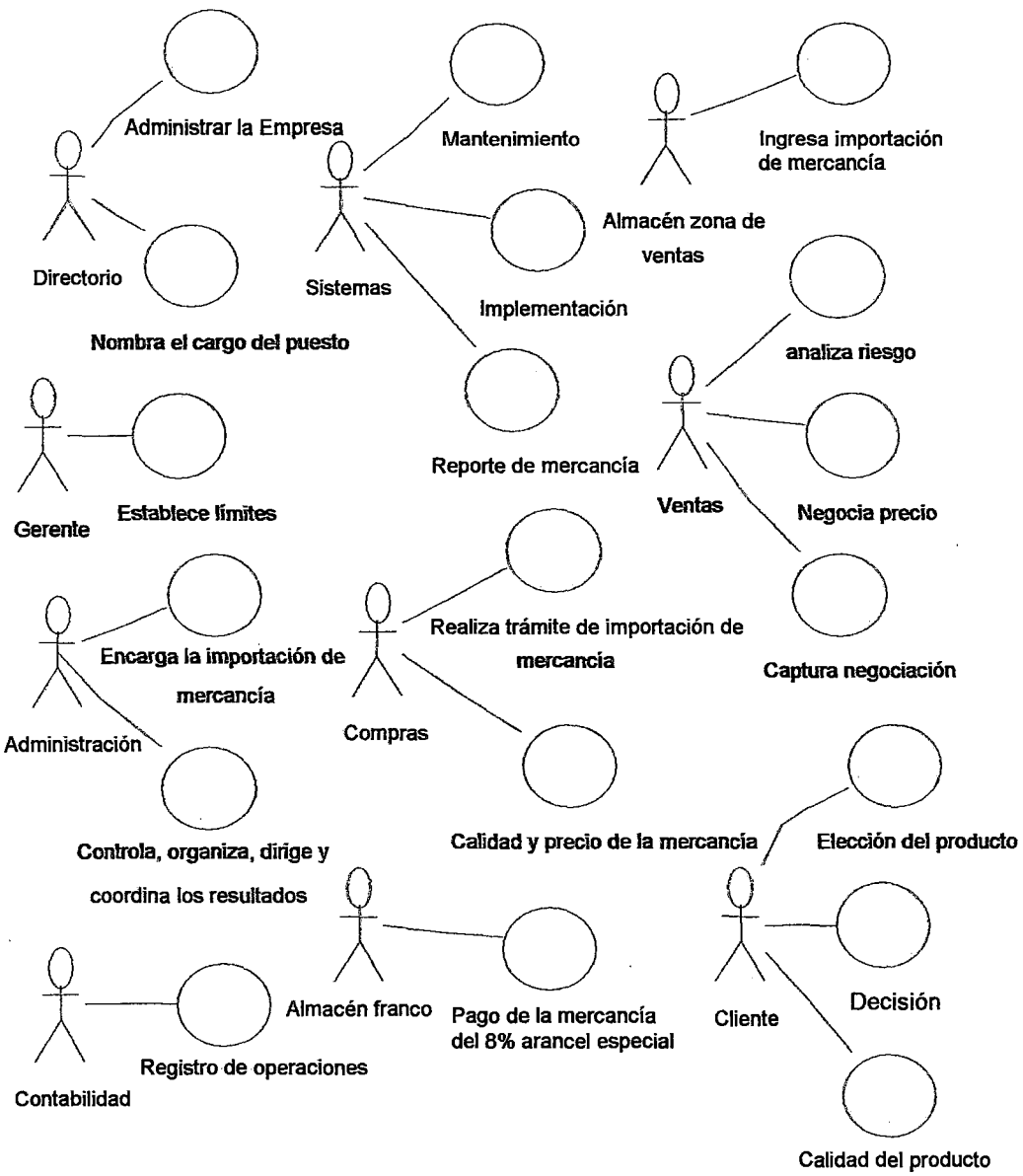
Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen

virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch, puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación.

5.26. Modelado de objetos funciones de la Empresa



5.27. Revisión de controles de los procesos informáticos

Una vez conseguida la operatividad de los sistemas, el segundo objetivo de la auditoría es la verificación de la observancia, de las normas teóricamente existentes en el departamento de informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

- Las normas generales de la instalación informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa sobre todo, verificando que esta normativa general informática no esté en contradicción con alguna norma general no informática de la empresa.
- Los procedimientos generales informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de explotación. Tampoco el alta de una nueva aplicación podría producirse si no existieran los procedimientos de backup y recuperación correspondientes.
- Los procedimientos específicos informáticos. Igualmente, se revisará su existencia en las áreas fundamentales. Del mismo modo, deberá comprobarse que los Procedimientos

Específicos no se opongan a los procedimientos generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los procedimientos generales de la propia empresa, a los que la informática debe estar sometida.

5.28. Intranet

Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización, parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a Internet, una red entre organizaciones, haciendo referencia por contra a una red comprendida en el ámbito de una organización.

Funciones de la intranet

Tiene como función principal proveer lógica de negocios para aplicaciones de captura, informes y consultas con el fin de facilitar la producción de dichos grupos de nivel de grupo de trabajo. Las redes internas corporativas son potentes herramientas que permiten divulgar información de la compañía a los empleados con efectividad, consiguiendo que éstos estén permanentemente informados con las últimas novedades y datos de la organización.

Tienen gran valor como repositorio documental, convirtiéndose en un factor determinante para conseguir el objetivo de la oficina sin papeles. Añadiéndoles funcionalidades como un buen buscador y una organización adecuada, se puede conseguir una consulta rápida y eficaz por parte de los empleados de un volumen importante de documentación. Los beneficios de una intranet pueden ser enormes. Estando tal cantidad de información al alcance de los empleados ahorrarán mucho tiempo buscándola.

Las intranet también deberían cumplir unos requisitos de accesibilidad web, permitiendo su uso a la mayor parte de las personas, independientemente de sus limitaciones físicas o las derivadas de su entorno. Gracias a esto, promueven nuevas formas de colaboración y acceso a los sistemas. Ya no es necesario reunir a todos en una sala para discutir un proyecto.

5.29. Definición de la auditoría de sistemas

Es un examen objetivo, sistemático y profesional de evidencias, realizado con el fin de proporcionar una evaluación independiente sobre el desempeño de los sistemas utilizados en una entidad, programa o actividad.

La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.

El examen y evaluación de los procesos del área de procesamiento automático de datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas informáticos en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.

El proceso de recolección y evaluación de evidencia para determinar si un sistema automatizado:

Daños, salvaguarda activos, destrucción, uso no autorizado, robo, mantiene integridad de información precisa, los datos completa, oportuna, confiable, alcanza metas, contribución de la organización, la función informática, consume recursos, utiliza los recursos adecuadamente, eficientemente en el procesamiento de la información.

5.30. Características de la auditoría de sistemas

Del mismo modo, los sistemas informáticos o tecnológicos han de protegerse de modo global y particular: a ello se debe la existencia

de la auditoría de sistemas para el desarrollo de los procesos informáticos.

Síntomas de necesidad de una auditoría de sistemas:

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

- Síntomas de descoordinación y desorganización:

  No coinciden los objetivos de la informática de la compañía y de la propia compañía.

  Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

- Síntomas de mala imagen e insatisfacción de los usuarios:
  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
  - No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

- Síntomas de debilidades económico-financieras:
  - Incremento desmesurado de costes.
  - Necesidad de justificación de inversiones informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
  - Desviaciones presupuestarias significativas.
  - Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a desarrollo de proyectos y al órgano que realizó la petición).
- Síntomas de inseguridad: Evaluación de nivel de riesgos:
  - Seguridad lógica.
  - Seguridad física.
  - Confidencialidad.

Centro de proceso de datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón

por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

5.31. Objetivos de la auditoría de sistemas

- Evaluar la fiabilidad.
- Evaluar la dependencia de los sistemas y las medidas tomadas para garantizar su disponibilidad y continuidad.
- Revisar la seguridad de los entornos y sistemas.
- Analizar la garantía de calidad de los sistemas de información.
- Analizar los controles y procedimientos tanto organizativos como operativos.
- Verificar el cumplimiento de la normativa y legislación vigentes.
- Elaborar un informe externo independiente.

5.32. Objetivos para una buena gestión de los sistemas de la información en la empresa

- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información.
- Seguridad del personal, los datos, el hardware, el software y las instalaciones.
- Minimizar existencias de riesgos en el uso de tecnología de información.

- Conocer la situación actual del área informática para lograr los objetivos.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad de los entornos.
- Incrementar la satisfacción de los usuarios de los sistemas informáticos.
- Capacitación y educación sobre controles en los sistemas de información.
- Buscar una mejor relación costo-beneficio de los sistemas automáticos.
- Decisiones de inversión y gastos innecesarios.

5.33. Alcance de la auditoría de sistemas

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el informe final, de modo que quede perfectamente determinado, no solamente hasta qué puntos se ha llegado, sino cuáles materias fronterizas han sido omitidas.

5.34. Función de la auditoría de sistemas

Es promover la adecuación, revisión, evaluación y recomendaciones para el mejoramiento de los controladores internos en los sistemas de información de la empresa, así como evaluar la utilización de los recursos humanos, materiales y tecnológicos envueltos en el procesamiento de los mismos.

La función de la auditoría de sistemas debe ser absolutamente independiente; no tiene carácter ejecutivo ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades; estas sugerencias plasmadas en el informe final reciben el nombre de recomendaciones.

5.35. Papel de la auditoría de sistemas

La auditoría nace como un órgano de control de algunas instituciones estatales y privadas. Su función es estrictamente económico - financiera, y los casos inmediatos se encuentran en los estrados judiciales y las contrataciones de contadores expertos por parte de bancos oficiales.

La función de auditoría debe ser absolutamente independiente; la auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y deficiencias. Aunque pueden aparecer sugerencias y planes de acción para eliminar las deficiencias y debilidades antes dichas; estas sugerencias plasmadas en el informe final reciben el nombre de recomendaciones.

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que el auditor tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los sistemas, unidos a los plazos demasiados breves de los que suelen disponer para realizar su tarea.

El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.

5.36. Justificativos para efectuar una auditoría de sistemas

- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos).

- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados con los equipos informáticos.
- Falta de una planificación informática.
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del recurso humano.
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.
- Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción.

5.37. Evaluación de la auditoría de sistemas

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

elaborados sin el adecuado señalamiento de prioridades y de objetivos.

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

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

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

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

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

5.38. Evaluación del análisis

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

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

- La planeación estratégica: agrupadas las aplicaciones en conjuntos relacionados entre sí y no como programas aislados. Las aplicaciones deben comprender todos los sistemas que puedan ser desarrollados en la dependencia, independientemente de los recursos que impliquen su desarrollo y justificación en el momento de la planeación.
- Los requerimientos de los usuarios.

- El inventario de sistemas en proceso al recopilar la información de los cambios que han sido solicitados, sin importar si se efectuaron o se registraron.

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

- Planeada para ser desarrollada en el futuro.
- En desarrollo.
- En proceso, pero con modificaciones en desarrollo.
- En proceso con problemas detectados.
- En proceso sin problemas.
- En proceso esporádicamente.

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

Es importante revisar la situación en que se encuentran los manuales de análisis y si están acordes con las necesidades de la dependencia. En algunas ocasiones se tiene una microcomputadora, con sistemas sumamente sencillos y se solicita que se lleve a cabo una serie de análisis que después hay que

plasmar en documentos señalados en los estándares, lo cual hace que esta fase sea muy compleja y costosa. Los sistemas y su documentación deben estar acordes con las características y necesidades de una dependencia específica.

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

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

5.39. Evaluación del diseño lógico del sistema

Una vez que se ha analizado estas partes, se deberá estudiar la participación que tuvo el usuario en la identificación del nuevo sistema, la participación de auditoría interna en el diseño de los

controles y la determinación de los procedimientos de operación y decisión.

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

Los puntos a evaluar son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos (antes y después del proceso electrónico de datos).
- Proceso lógico necesario para producir informes.
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.

- Sistemas de control.
- Responsables.
- Número de usuarios.

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

- Manual del usuario.
- Descripción de flujo de información y/o procesos.
- Descripción y distribución de información.
- Manual de formas.
- Manual de reportes.
- Lista de archivos y especificaciones.

5.40. Evaluación del desarrollo del sistema

En esta etapa del sistema se deberán auditar los programas, su diseño, el leguaje utilizado, interconexión entre los programas y características del hardware empleado (total o parcial) para el desarrollo del sistema. Al evaluar un sistema de información se tendrá presente que todo sistema debe proporcionar información para planear, organizar y controlar de manera eficaz y oportuna, para reducir la duplicidad de datos y de reportes y obtener una mayor seguridad en la forma más económica posible. De ese modo contará con los mejores elementos para una adecuada toma de decisiones. Al tener un proceso distribuido, es preciso considerar la

seguridad del movimiento de la información entre nodos. El proceso de planeación de sistemas debe definir la red óptima de comunicaciones, los tipos de mensajes requeridos, el tráfico esperado en las líneas de comunicación y otros factores que afectan el diseño. Es importante considerar las variables que afectan a un sistema: ubicación en los niveles de la organización, el tamaño y los recursos que utiliza. Las características que deben evaluarse en los sistemas son:

- Dinámicos (susceptibles de modificarse).
- Estructurados (las interacciones de sus componentes o subsistemas deben actuar como un todo).
- Integrados (un sólo objetivo). En él habrá sistemas que puedan ser interrelacionados y no programas aislados.
- Accesibles (que estén disponibles).
- Necesarios (que se pruebe su utilización).
- Comprensibles (que contengan todos los atributos).
- Oportunos (que esté la información en el momento que se requiere).
- Funcionales (que proporcionen la información adecuada a cada nivel).

- Estándar (que la información tenga la misma interpretación en los distintos niveles).
- Modulares (facilidad para ser expandidos o reducidos).
- Jerárquicos (por niveles funcionales).
- Seguros (que sólo las personas autorizadas tengan acceso).
- Únicos (que no duplique información).

5.41. Seguridad lógica

Los equipos informáticos son instrumentos que guardan gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de ésta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad informática.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

El llamado ""virus informáticos", tiene diferentes intenciones que se encuentra principalmente por paquetes que son copiados sin

autorización ("piratas") y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de los equipos informáticos comienza desde la utilización para usos ajenos de la organización, la copia de programas para fines de comercialización, sin reportar los derechos de autor, hasta el acceso por vía telefónica a bases de datos, a fin de modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas informático, es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de los equipos informáticos grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.

- Organización y división de responsabilidades.
- Seguridad física y contra catástrofes (incendio, terremotos, y otros).
- Prácticas de seguridad del personal.
- Elementos técnicos y procedimientos.
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales).
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos.
- El papel de los auditores, tanto internos como externos.
- Planeación de programas de desastre y su prueba.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio, entre el costo por pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).

Identificar aquellas aplicaciones que tengan un alto riesgo.

Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.

Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medias preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.

Hay que tener mucho cuidado con la información que sale de la oficina.

Para clasificar la instalación en términos de riesgo se debe:

Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.

Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.

Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente

afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

- Especificar la aplicación, los programas y archivos.
- Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.
- Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.
- En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de la organización.
  - El personal que prepara la información no debe tener acceso a la operación.
  - Los análisis y programadores no deben tener acceso al área de operaciones y viceversa.
  - Los operadores no debe tener acceso irrestringido a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.

- Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar sistemas de seguridad puede, reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

5.42. Seguridad física

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo. Entre las precauciones que se deben revisar están:

- Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan.

Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.
- Los materiales más peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

5.43. El control interno en la auditoría de sistemas

Básicamente todos los cambios que se realizan en una organización someten a una gran tensión a los controles internos existentes.

Cuando un auditor profesional se somete a auditar una empresa, lo primero que se le viene a la cabeza es mejorar todos los procesos que se llevan en la misma para buscar la eficiencia total. Este trabajo no se hace de la noche a la mañana; para ello se empieza ya bien sea por áreas o departamentos o mejor dicho se empieza a trabajar internamente.

La mayoría de las organizaciones han acometido varias iniciativas en tal sentido tales como:

- La reestructuración de los procesos empresariales.
- La gestión de la calidad total.
- El redimensionamiento por reducción y/o por aumento de tamaño hasta el nivel correcto.
- La contratación externa.
- La descentralización.

5.44. Las funciones del control interno en la auditoría de sistemas

El control interno en la auditoría de sistemas controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización y/o la dirección informática, así como los requerimientos legales.

La función del control interno en la auditoría de sistemas es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Control interno en la auditoría de sistemas suele ser un órgano staff de la dirección del departamento de informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de la auditoría de informática, así como de las auditorias externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los graso adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y responsabilidad del logro de esos niveles se ubique exclusivamente en la función de control interno, si no que cada responsable de

objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

La auditoria de sistemas es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los eficazmente los fines de la organización y utiliza eficiente mente los recursos.

5.45. Diferencias y similitudes entre el control interno y la auditoría de sistemas

DESCRIPCIÓN	CONTROL INTERNO	AUDITOR DE SISTEMAS
SIMILITUDES	PERSONAL INTERNO Conocimientos especializados en tecnologías de información verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la dirección informática y la dirección general para los sistemas de información.	
DIFERENCIAS	Análisis de los controles en el día a día. Informa a la dirección del departamento de informática sólo personal interno el enlace de sus funciones es únicamente sobre el departamento de informática.	Análisis de un momento informático determinado. Informa a la dirección general de la organización. Personal interno y/o externo tiene cobertura sobre todos los componentes de los sistemas de información de la organización.

5.46. Definición y tipo de controles internos

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para lograr o conseguir sus objetivos.

Los controles internos se clasifican en los siguientes:

- **Controles preventivos:** Para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- **Controles detectivos:** Cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones.
- **Controles correctivos:** Facilitan la suelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

5.47. Implantación de un sistema de controles internos informáticos

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- **Entorno de red:** Esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.
- **Configuración del ordenador base:** Configuración del soporte físico, en torno del sistema operativo, software con particiones, entornos (pruebas y real), y las bibliotecas de los programas.
- **Entorno de aplicaciones:** Procesos de transacciones, sistemas de gestión de base de datos y entornos de procesos distribuidos.
- **Productos y herramientas:** Software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

- **Seguridad del ordenador base:** Identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, y otros.

Para la implantación de un sistema de controles internos informáticos habrá que definir:

- **Gestión de sistema de información:** Políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.
- **Administración de sistemas:** Controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.
- **Seguridad:** Incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.
- **Gestión del cambio:** Separación de las pruebas y la producción a nivel del software y controles de procedimientos para la migración de programas software aprobados y probados.

5.48. Seguridad en el uso de los equipos informáticos

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro de la oficina informática, se conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

- Se debe restringir el acceso a los programas y a los archivos.
- Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
- Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
- No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
- Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
- Se deben monitorear periódicamente el uso que se le está dando a las terminales.
- Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

- El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.
- Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
- Debe controlarse la distribución de las salidas (reportes, cintas, y otros).
- Se debe guardar copias de los archivos y programas en lugares ajenos al centro de informático y en las instalaciones de alta seguridad.
- Se debe tener un estricto control sobre el acceso físico a los archivos.
- En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice los equipos informáticos para trabajos personales. Otro de los puntos en los que hay que tener seguridad

es en el manejo de información. Para controlar este tipo de información se debe:

- Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
- Sólo el personal autorizado debe tener acceso a la información confidencial.
- Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.
- Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- Equipo, programas y archivos.
- Control de aplicaciones por terminal.
- Definir una estrategia de seguridad de la red y de respaldos.
- Requerimientos físicos.

- Estándar de archivos.
- Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

5.49. Seguridad al restaurar los equipos informáticos

En un mundo que depende cada día más de los servicios proporcionados por las equipos informáticos, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

- En algunos casos es conveniente no realizar alguna acción y reanudar el proceso.
- Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.
- El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo, al punto de tener la seguridad del contenido del mismo, a partir de él reanudar el proceso.
- Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.
- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia, deberá ser planeado y probado previamente.

Este grupo de emergencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, el nivel de servicio planeado y su influjo en la operación de la organización.

Además de los procedimientos de recuperación y reinicio de la información, se deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.

5.50. Procedimientos de respaldo en caso de desastre

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema informático.

El sistema debe ser probado y utilizado en condiciones anormales, para que en casó de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.

La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se ha de utilizar respaldos.

Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco y otros.

El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.

En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia. La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración

de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.

Los desastres que pueden suceder podemos clasificar así:

- Completa destrucción de los equipos informáticos.
- Destrucción parcial de los equipos informáticos.
- Destrucción o mal funcionamiento de los equipos auxiliares del centro informático (electricidad, aire, acondicionado, y otros).
- Destrucción parcial o total de los equipos descentralizados.
- Pérdida total o parcial de información, manuales o documentación.
- Pérdida del personal clave.
- Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

- La documentación de programación y de operación.
- Los equipos:
  - El equipo completo.
  - El ambiente de los equipos.
  - Datos y archivos.
  - Papelería y equipo accesorio.

- Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- Asegurarse de que todos los miembros sean notificados.
- informar al director de informática.
- Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que parte del plan debe ser activada.
- Determinar el estado de todos los sistemas en proceso.
- Notificar a los proveedores del equipo cual fue el daño.
- Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:
  - Elaboración de una lista con los métodos disponibles para realizar la recuperación.

- Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).
- Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.
- Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

- Posponer las aplicaciones de prioridad más baja.
- Cambiar la frecuencia del proceso de trabajos.
- Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.

Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo.

Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, y otros,

a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

- Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- Se debe tener documentados los cambios de software.
- En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- Configuración de equipos.
- Configuración de equipos de captación de datos.
- Sistemas operativos.
- Configuración de equipos periféricos.

CONCLUSIONES

1. Los procesos informáticos inciden desfavorablemente al aplicar una Auditoría de Sistemas en la Gestión Administrativa de la Empresa AMDIRESA, período 2009.
2. Por lo tanto en la organización de los equipos informáticos el mantenimiento correctivo y preventivo, no se desarrolla de forma eficiente.
3. En el control de los procesos informáticos los sistemas de información no se usan de forma adecuada para tener una óptima información.
4. En la seguridad informática sea lógica y física no son aplicados en los equipos informáticos que tiene la Empresa.
5. En la evaluación tecnológica de los procesos informáticos; ya que la tecnología de información, desarrollo y soporte no se desarrolla de forma óptima.
6. El plan de sistemas de información; ya que la elaboración y programación no se desarrollo de forma eficiente en la Empresa.

RECOMENDACIONES

Se propone realizar una Auditoría de Sistemas, con el propósito de mejorar los procesos informáticos y de esta forma optimizar la gestión administrativa de la Empresa AMDIRESA, período 2009.

REFERENCIAS BIBLIOGRÁFICAS

1. Bravo Cervantes, Miguel H. (1995). Auditoria del sistema informático; (2da. Edición). Lima – Perú.
2. Ferreyros Morón, Juan A. (2008). Informática SIG y Auditoria de Sistemas; (2da. Edición). Lima – Perú.
3. Gutiérrez Melo, Julián. (2009). La seguridad física de los equipos informáticos. Colombia.
4. Gil Pechuan, Ignacio. (1994). Sistemas y tecnologías de la información para la gestión. (2da. Edición). México: (Editorial McGraw Hill).
5. Gorje, Ferry. (2011). Principio de Administración. (3era. Edición). Monterrey – México.
6. Koontz Harold. (2011). Elementos de la Administración. (3era. Edición). México (Editorial Mc Graw – Hill Interamericana).
7. Kendall Kendall. (1991). Análisis y Diseño de Sistemas; (2da. Edición).
8. Martín James. (2006). Sistema de información y administración; (Editorial MacGraw Hill).

9. M., Scout George. (2000). Sistemas de información y la toma de decisiones; (Editorial McGraw – Hill).

10. Olson, Margrethe H. (2008) Principios de Sistemas de Información; (2da. Edición). Editorial McGraw - Hill.

11. Reyes Ponce, Agustín. (2010). Sistema de Administración. (4ta. Edición). Colombia.

12. Robert Murdick y Joel Ross. (2011). Gerencia de Información. (2da. Edición). EEUU

13. Rojas, Enrique Jofré. (2001). Modelo de Diseño y ejecución de estrategias de negocios. (2da. Edición). Universidad de Chile.

14. R, Mauricio Solano R. (2008). Auditoría de Sistemas. (4ta. Edición). Monterrey – México.

15. S, Alice Naranjo. (2010). Auditoría de Sistemas. (2da. Edición). Guayaquil – Ecuador.

16. Senn, James A. (1993). Análisis y diseño de sistemas de información. (3era. Edición). Ediciones McGraw Hill.

MANUALES

17. Asociación de la Tecnología de Información de América (ITAA). (2011).
18. COSO II. (2004). Manual "Gestión de Riesgos Corporativos – Técnicas de Aplicación".
19. COBIT 4.0. (2009). Manual Informático; España.
20. I.E.E.E. Manual de función de informática. (2008). Estados Unidos.
21. ISACA. (2010). Manual de Auditoría de Sistemas; Perú.
22. INEI. (2011). Manual de Auditoría de Sistemas; Perú.
23. Pontificia Universidad Católica. (2006). Manual de auditoría de sistemas. Chile.
24. Recursos Informáticos de las entidades del gobierno central de Panamá. (2006).
25. Universidad San Martín de Porres. (2009). Manual de Auditoría de Sistemas. Lima – Perú.
26. Universidad Vasco. (2010). Manual de Auditoría de Sistemas. España.

NORMAS

27. Norma de Control Interno RC – 072 – 98 – CG.

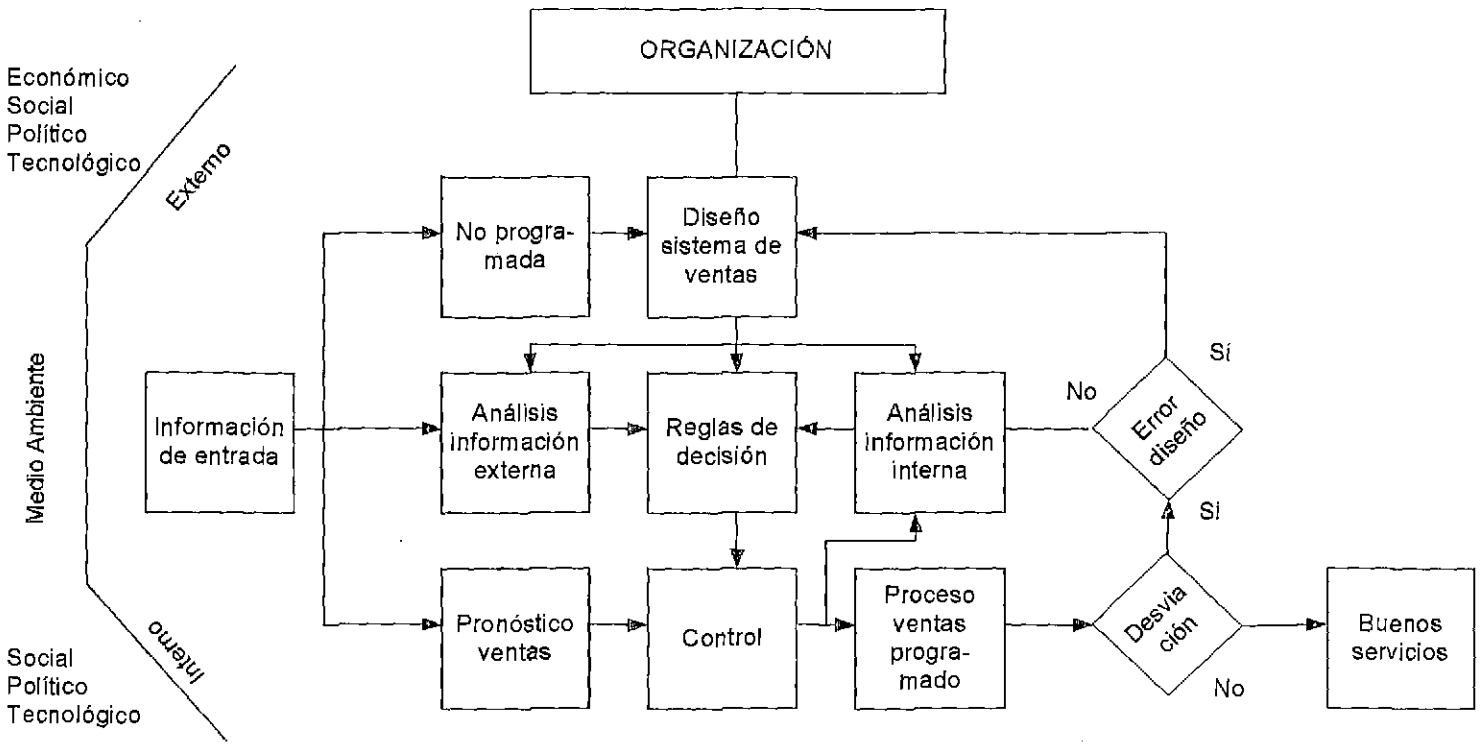
MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVO	HIPÓTESIS	CONCLUSIONES	RECOMENDACIONES
1. Problema General ¿De qué manera la evaluación de los procesos informáticos a través de la auditoría de sistemas influye en la gestión administrativa de la empresa AMDIRESA?, período 2009.	**1. Objetivo General** Evaluar si los procesos de informáticos a través de la auditoría de sistemas influyen en la gestión administrativa de la empresa AMDIRESA, período 2009.	**1. Hipótesis General** La evaluación de los procesos de informáticos a través de la auditoría de sistemas incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.	**Conclusión General** Los procesos informáticos inciden desfavorablemente al aplicar una auditoría de sistemas en la gestión administrativa de la empresa AMDIRESA, período 2009.	Se propone realizar una auditoría de sistemas, con el propósito de mejorar los procesos informáticos y de esta forma optimizar la gestión administrativa de la empresa AMDIRESA, período 2009.
2. Problemas Específicas	**2. Objetivos Específicos**	**2. Hipótesis Específicos**	**Conclusiones Específicas**	
a. ¿De qué manera la organización de los equipos informáticos influye en la gestión administrativa de la empresa AMDIRESA?, período 2009.	a. Verificar si la organización de los equipos informáticos influye en la gestión administrativa de la empresa AMDIRESA, período 2009.	a. La organización de los equipos informáticos influye significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.	Por lo tanto en la organización de los equipos informáticos el mantenimiento correctivo y preventivo, no se desarrolla de forma eficiente.	
b. ¿Cómo el control de los procesos informáticos influye en la gestión administrativa de la empresa AMDIRESA?, período 2009.	b. Analizar si el control de los procesos informáticos influye en la gestión administrativa de la empresa AMDIRESA, período 2009.	b. El control de los procesos informáticos incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.	En el control de los procesos informáticos los sistemas de información no se usan de forma adecuada para tener una óptima información.	

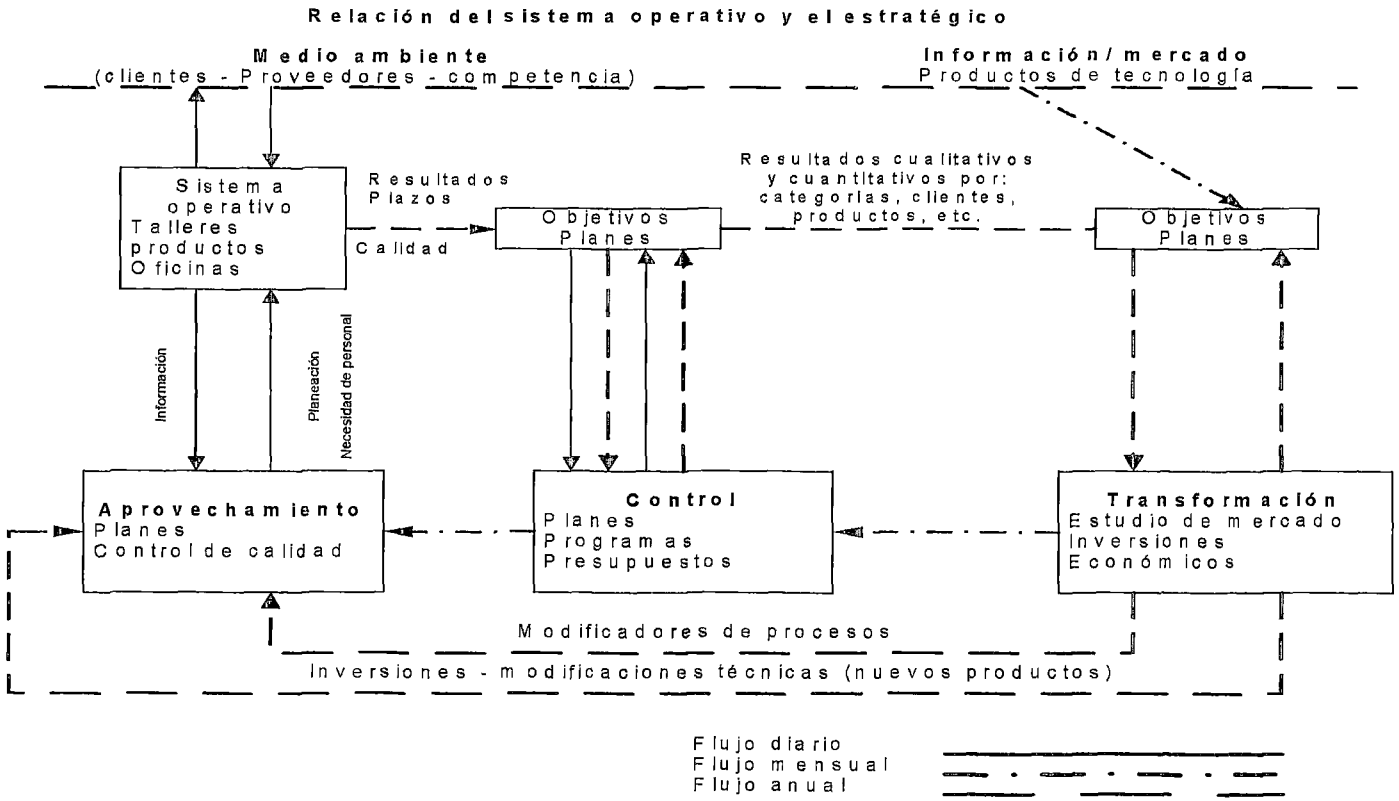
MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVO	HIPÓTESIS	CONCLUSIONES	RECOMENDACIONES
c. ¿En qué medida la seguridad informática influyen en la gestión administrativa de la empresa AMDIRESA?, período 2009.	c. Establecer si la seguridad informática influyen en la gestión administrativa de la empresa AMDIRESA, período 2009.	c. La seguridad informática incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.	En la seguridad informática sea lógica y física no son aplicados en los equipos informáticos que tiene la Empresa.	
d. ¿De que manera la evaluación tecnológica de los procesos informáticos incide en la gestión administrativa de la empresa AMDIRESA?, período 2009.	d. Elaborar si la evaluación tecnológica de los procesos informáticos incide en la gestión administrativa de la empresa AMDIRESA, período 2009.	d. La elaboración de una evaluación tecnológica de los procesos informáticos influye significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.	En la evaluación tecnológica de los procesos informáticos; ya que la tecnología de información, desarrollo y soporte no se desarrolla de forma óptima.	
e. ¿De qué manera el plan de sistemas de información incide en la gestión administrativa de la empresa AMDIRESA?, período 2009.	e. Revisar si el plan de sistemas de información Incide en la gestión administrativa de la empresa AMDIRESA, período 2009.	e. El plan de sistema de información incide significativamente en la gestión administrativa de la empresa AMDIRESA, período 2009.	El plan de sistemas de información; ya que la elaboración y programación no se desarrollo de forma eficiente en la Empresa	

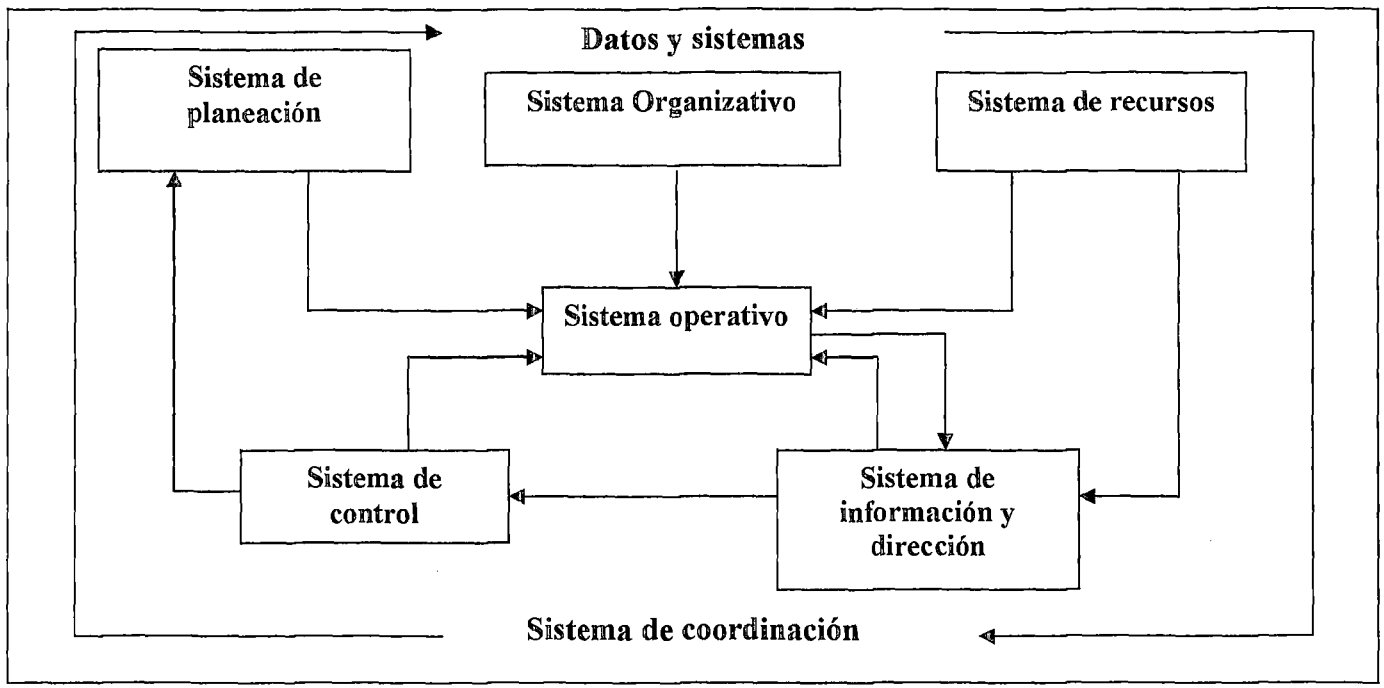
Anexo 01: Organización interna



Anexo 02: Organización externa



Anexo 03: Propiedades de datos y de sistemas



Anexo 04: Escala de fiabilidad

Resumen del procesamiento de los casos

Descripción		N	%
Casos	Validos	23,00	100,00
	Excluidos	0,00	0,00
	Total	23,00	100,00

a. Eliminación por lista basada en todas las variables del procedimiento..

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
0,973	8,00