PROPUESTA DE UNA METODOLOGIA DE AUDITORIA INFORMATICA PARA LA REVISION DE SISTEMAS DE INFORMACION BARQUISIMETO 2011

MANUEL DE JESÚS CRESPO GÓMEZ

MAILEN YELITZA CAMACARO RIVAS

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"

BARQUISIMETO, 2011.

PROPUESTA DE UNA METODOLOGIA DE AUDITORIA INFORMATICA PARA LA REVISION DE SISTEMAS DE INFORMACION BARQUISIMETO 2011

POR

MANUEL DE JESÚS CRESPO GÓMEZ

MAILEN YELITZA CAMACARO RIVAS

Trabajo de Ascenso presentado para optar a la Categoría de Asociado en el escalafón del personal Docente y de Investigación

UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"
Decanato de Ciencias y Tecnología

BARQUISIMETO, 2011.

DEDICATORIA

A *Dios Todopoderoso*, quien
ilumina y protege todos los días de nuestras vidas.

A nuestras familias y amigos,
por su constante apoyo.

Manuel Crespo Mailen Camacaro..

AGRADECIMIENTO

A los estudiantes de la asignatura Auditoría Informática, por su participación.

A la comunidad del Decanato de Ciencias y Tecnología.

A todos... ¡ nuestro más sincero agradecimiento !

ÍNDICE GENERAL

UNIVERSIDAD CENTROCCIDENTAL LISANDRO ALVARADO
VICE-RECTORADO ACADÉMICO
DECANATO DE CIENCIAS Y TECNOLOGÍA

PROPUESTA DE UNA METODOLOGIA DE AUDITORIA INFORMATICA PARA LA REVISION DE SISTEMAS DE INFORMACION

AUTORES: Manuel Crespo Gómez.
Mailen Camacaro Rivas

AÑO : 2011

RESUMEN

La Auditoria Informática ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información ya que las mismas utilizan la informática para gestionar sus “negocios” de forma rápida y eficiente con el fin de obtener beneficios económicos y de costes. De allí la necesidad de disponer de un metodología adecuada para la ejecución de las Auditorias Informáticas. El objetivo General de la Investigación es Diseñar una Metodología de Auditoria Informática para la revisión de los Sistemas de Información. El Marco Teórico, está sustentado en aspectos tales como: Evolución de la Auditoria, Importancia, Principios de Auditoria, Tipos, Perfil del auditor, Normas, Pruebas de Auditoria, Fases de la Auditoria, Conocimiento Preliminar de los Controles Internos, Las Evidencias de Auditoria, Normas de Auditoria, Técnicas y herramientas de la auditoria, Planes de contingencia, Estructura del informe, Características, Sistemas de Información, los riesgos potenciales, la seguridad física, generalidad de la seguridad en el área de la teleinformática, técnicas y herramientas relacionadas con la seguridad de datos y software de aplicación, programas,

objetivos y criterios de la auditoria en el área de la teleinformática etc. Además de la revisión de las leyes relacionadas con la tecnología informática y la auditoria. El estudio se ubica dentro del tipo de Investigación analítico descriptivo y explicativo y con estudio de campo. Se aplicaron instrumentos de observación directa y cuestionario para obtener datos, software de simulación. Se incluye el Análisis e Interpretación de los Datos y las Conclusiones y Recomendaciones. Finalmente se presenta la Metodología de Auditoria Informática propuesta.

Descriptores de Contenido: Tecnología Informática, Sistemas de Información, Auditoria Informática.

INTRODUCCIÓN

En los actuales momentos, la globalización ha creado efectos sobre los distintos escenarios del quehacer diario de las organizaciones, siendo éstos más dinámicos, sometidos constantemente a cambios, innovaciones y turbulencias, en el que las instituciones se ven expuestas a procesos invariables de permutas, que ameritan una gerencia eficaz que permita optimizar los procesos que se llevan a cabo dentro de ellas, donde deben existir líderes capaces de tomar decisiones adecuadas y oportunas, proactivos y dispuestos a implementar herramientas y tecnologías de punta que lo apoyen en la difícil tarea de lograr la excelencia organizacional.

Con base en lo antes expuesto, el éxito de la organización para alcanzar sus objetivos depende, en gran medida, del desempeño gerencial de la misma, de sus procesos y de cómo se ejecutan éstos con miras a elevar la calidad en la prestación de servicio y atención al usuario, para lo cual deben existir estrategias que permitan enfrentar de manera exitosa los actuales y futuros escenarios para la empresa, logrando esto mediante el diseño de acciones, metas y objetivos, aunados a una buena filosofía de gestión y un capital humano bien motivado para su ejecución.

Es así, como mediante este estudio se pretende generar un aporte a objeto de que las organizaciones puedan evaluar el uso de sus sistemas de información y el impacto que este uso tiene en su efectividad organizacional, la auditoría informática puede convertirse en una actividad que permita descubrir como las empresas usan sus sistemas organizacionales. De allí la importancia de proponer una metodología de auditoría informática que pueda ser aplicada.

El trabajo que se presenta se encuentra estructurado en seis (6) capítulos; denominándose el primero, El Problema, el cual contiene el planteamiento del mismo, se establecen los objetivos del estudio y su justificación. El segundo denominado Marco Teórico, en el que se

presenta la revisión bibliográfica y consta de los antecedentes, bases teóricas, definición de términos básicos y aspectos legales. En el tercero, se expone el Marco Metodológico, en el que se describe la Naturaleza de la Investigación, Población y Muestra, Técnicas e Instrumentos de Recolección de Datos, técnicas de Procesamiento y Análisis de los Datos y conceptualización y operacionalización de la variable en estudio. El cuarto se denomina Análisis e Interpretación de los Resultados donde se muestra el desarrollo de cada uno de los objetivos específicos planteados, a través de la aplicación de los instrumentos; el quinto describe la metodología de auditoría informática propuesta y el Capítulo VI, llamado Conclusiones y Recomendaciones. Por último; se exponen las Referencias Bibliográficas y Anexos, para lograr una mayor comprensión por parte del lector sobre la investigación.

CAPITULO I

EL PROBLEMA

Planteamiento y Formulación del Problema

Los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, como lo es la información.

Los Sistemas de Información de la Empresa**,** cuyos objetivos principales son la automatización de los procesos operativos, proporcionan información que sirve de apoyo para la toma de decisiones y contribuyen a lograr ventajas competitivas a través de su implantación y uso.

La Informática hoy, es un proceso vital en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a las necesidades de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa, ayudan a la toma de decisiones.

En tal sentido el proceso tecnológico de una empresa, tanto pública como privada, va en sintonía con la operatividad de la misma, es decir la administración de una empresa tal y como lo plantea Stoner, Gilberth y Freedman (1996), que es el "proceso de planear, organizar, liderizar y controlar el trabajo de los miembros de la organización y de utilizar todos los recursos disponibles de la empresa para alcanzar objetivos organizacionales establecidos", plantea que la optimización de los procesos va en función de la racionalidad en el uso de los recursos con se cuenta, en tal sentido la tecnología cobra mayor importancia, toda vez que la misma proporciona las herramientas necesarias para contribuir al éxito de toda organización, es decir con sistemas de Información precisos y oportunos la administración de cualquier empresa puede hacer el seguimiento necesario para evaluar y controlar el progreso de sus planes,

objetivos y metas y por otra parte pueden servir de apoyo al proceso de toma de decisiones y permiten que tanto la planificación, el control y las operaciones se realicen eficazmente.

Por ende, debido a la importancia de los Sistemas de Información en el funcionamiento de una empresa, existe la Auditoria Informática.

El término de Auditoria se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas.

El concepto de auditoria es mucho más que esto, si bien es un examen el mismo es crítico y su fin principal es evaluar la eficacia y eficiencia de una parte, área o sección de un organismo, una entidad etc.

El Boletín de Normas de auditoria del Instituto mexicano de contadores nos dice: “La auditoria no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo son de carácter indudable.”

De todo esto se puede deducir que la auditoria es un examen crítico pero no mecánico, que el mismo no implica la presunción de la existencia de fallas en el ente auditado y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Estos dos temas importantes Informática y Auditoria, puede decirse que están unidos entre sí, pues si existe en una organización la necesidad de evaluar los Sistemas de Información, motivado a que los mismos puedan cubrir en un momento dado las expectativas o no para la que fueron creados, surge la interrogante ¿Por qué y para qué evaluarlos?, se hace necesario entonces aplicar una Auditoria Informática.

La auditoria Informática tiene entre otros como objetivos principales el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos y una de las Bases que impulsa el presente Trabajo de Investigación, es definir una Metodología adaptada a la Cultura Venezolana que abarque elementos

de convergencia entre los modernos conceptos de auditoria de sistemas de información y los enfoques de auditoria tradicionales basados en el análisis de riesgos asociados a los procesos de negocio soportados en tecnología informática; esta metodología debe permitir identificar los objetivos de auditoria, planear y evaluar los ambientes de informática, evaluación del control y seguridad de la Información, desarrollo de pruebas y procedimientos de auditoria de sistemas, orientado a la administración del riesgo y su impacto sobre los procesos de la Organización, de manera de contar con métodos y prácticas que le permitan a las empresas estar concientes de la necesidad de contar con planes de contingencias y de continuidad del negocio que puedan asegurar la capacidad de responder a situaciones imprevistas que afecten el normal desempeño de las operaciones en el área de los Sistemas de Información, ya que en la actualidad las organizaciones han visto como la tecnología y las telecomunicaciones se han convertido en un elemento vital para su supervivencia y este cambio constante, brinda a la organización la posibilidad de soportar las decisiones de negocio y dirigir estrategias de inversión en Sistemas de Información para ser mucho mas competitivos, esto a generado cambios importantes en las organizaciones, el primero que el área de tecnología informática se convierta en un área estratégica y este a la par de las direcciones claves de la compañía; la segunda que el área de auditoria interna de la Organización, deba considerar la auditoria de Sistemas de Información como un aliado importante para el desarrollo de las actividades previstas a realizar dentro de su función de auditoria integral. Por lo tanto la auditoria de sistemas de información, poco a poco va adquiriendo una posición más robusta en la organización transformando la visión de antigua de los gerentes en identificarlo como un gasto innecesario, a la visión actual que lo posiciona como una INVERSIÓN.

Se hace necesario entonces plantearse una Metodología de Auditoria Informática para la revisión de los Sistemas de Información Organizacionales, que sirva de guía para quienes quieren incursionar en

el mundo de la evaluación de los sistemas de información, a través de la realización de auditorias pertinentes y oportunas. Surgen entonces las siguientes interrogantes:

- ¿Se hace necesario conocer la normativa legal que rige este proceso?
- ¿Se debe visualizar escenarios posibles susceptibles para la realización de una auditoria?
- ¿Se deben evaluar los riesgos potenciales y la seguridad de la información?
- ¿Deben identificarse los procedimientos sustantivos y de control a seguir para evaluar los sistemas de información?
- ¿Es necesario proponer una Metodología de auditoria para revisar los Sistemas de información?

A continuación se procederá al desarrollo de esta investigación a los fines de dar respuesta a las interrogantes anteriormente planteadas.

OBJETIVOS DE LA INVESTIGACIÓN

General

Diseñar una Metodología de Auditoria Informática para la revisión de los Sistemas de Información.

Específicos

(1) Conocer los aspectos legales que regulan la Auditoria Informática.
(2) Diagnosticar los escenarios posibles, analizar resultados **y** revisar los Sistemas de Información susceptibles para la realización de Auditorias Informáticas.
(3) Identificar los riesgos potenciales y la seguridad de información.
(4) Describir los procedimientos sustantivos y de control a seguir para la revisión de los sistemas de información.

(5) Proponer una Metodología de Auditoria para la revisión de los sistemas de información.

Justificación

La propuesta de una Metodología de Auditoria Informática, para la revisión de los Sistemas de Información constituye una herramienta valiosa, toda vez que definirá y aplicará controles en las diferentes áreas de la Informática como: instalaciones físicas, personal, teleinformática, seguridad en la información. Asimismo y evaluará el desempeño de las mismas áreas de la Informática y por otra parte proporciona aspectos teóricos prácticos que le dan apoyo, a través de Métodos y Procedimientos que permitan obtener un conjunto de herramientas sencillas que permitan ahondar en esta nueva área de análisis que comienza a surgir en el país.

También puede servir de apoyo e insumo para futuras investigaciones, además de que puede decirse que en el aspecto académico, puede ser guía para la enseñanza de la Auditoria Informática y para el sector profesional apoyaría a los profesionales en el área de la Informática y la Contaduría en el desarrollo y ejecución de una Auditoria Informática, por parte de los mismos.

A nivel del sector económico, apoyaría a empresas de diferentes sectores, proporcionándoles herramientas adecuadas para evaluar la eficiencia y eficacia de sus Sistemas de Información.

Desde el punto de vista práctico, proporcionaría las herramientas necesarias para la evaluación de los Sistemas de Información, presentando los controles, las pruebas y procedimientos de auditoria a seguir.

Esta investigación también puede servir de apoyo, ya que cumplirá con todo el proceso metodológico, necesario para poder desarrollar la misma.

CAPITULO II
MARCO TEÓRICO

Una vez planteados los objetivos general y específicos del presente trabajo de investigación, se presentan aspectos teóricos de interés tales como: Antecedentes de la investigación, dentro los cuales se analiza una serie de trabajos de investigación que abordan el proceso enseñanza-aprendizaje, además se presentan las Bases Teóricas que incluyen la revisión bibliográfica de temas sobre las Estrategia de Enseñanza Aprendizaje, los Sistemas de Información, la Auditoria Informática, los estándares de auditoría, aspectos legales entre otros.

Antecedentes

En la actualidad dado el avance vertiginoso de las tecnologías y las comunicaciones, existe una diversidad, de metodologías y herramientas que enriquecen el proceso de enseñanza-aprendizaje, en este sentido y debido a la importancia de esta investigación sobre Estrategias para el Proceso de Enseñanza-Aprendizaje de la asignatura Auditoria Informática, se hace necesario revisar los trabajos y teorías existentes y que puedan constituir un aporte valioso al presente trabajo.

Pernalete (2005), en su trabajo titulado "*El Desempeño Docente en el aula del Profesional de Informática bajo el Enfoque de Calidad*", tiene como objetivo analizar el desempeño docente en el aula del profesional de informática bajo el enfoque de calidad de la Universidad Pedagógica Experimental Libertador Instituto Pedagógico de Barquisimeto "Luis Beltrán Prieto Figueroa", con una investigación documental, modalidad monografía, a contextualizar la problemática del desempeño docente, tema de investigación que ha motivado a muchos autores y a instituciones por la importancia y efecto que produce en el ámbito sociocultural de cada país, y aún más si se desea que el desempeño docente se desarrolle con calidad. El estudio de la calidad en la Educación se puede

basar en diferentes modelos o enfoques entre ellos se encuentran el Modelo Heurístico de Enseñanza, Modelo de Gestión de Calidad en Educación, Enfoque Sistémico, Calidad de la Educación Orientado a la Calidad Total. Cada Modelo o enfoque persigue como meta mejorar el complejo sistema de enseñanza factor relevante para desarrollar un país y por ende mejorar la calidad de vida de cada ciudadano. La calidad del desempeño docente en el aula es estudiar la parte intrínsica del docente, es decir, personalidad, humor, cariño, valor, actitudes, etc., así como la parte administrativa de la enseñanza, la planificación, organización, control y seguimiento del conocimiento a impartir que permite incorporar mejoras a la educación, de esta manera el profesional de la informática incorporado a la docencia aporta soluciones en la educación, en virtud de que posee una preparación científica, técnica y humanística, capaces de proporcionar soluciones de calidad a los problemas relativos al tratamiento y gestión de la información en las instituciones, factor que ayuda a una enseñanza. Es de hacer notar que dicho trabajo de investigación, presenta una serie de estrategias, que en líneas generales constituye una base para la presente propuesta.

Mestra y Otros (2005), en su trabajo relacionado con las "*Estrategias didácticas para el desarrollo de competencias laborales específicas en la asignatura ingeniería Web del programa de ingeniería de sistemas de la corporación educativa mayor del desarrollo Simón Bolívar"*, manifiestan que el paradigma en el cual se enmarca la investigación es empírico analítico, pues con la misma se estudian estrategias didácticas que facilitan la eficacia en el quehacer de los docentes que imparten la asignatura Ingeniería Web del Programa de Ingeniería de Sistemas de la Corporación y por otra parte el estudio es de carácter descriptivo de las estrategias didácticas implementadas en el desarrollo de la cátedra de Ingeniería Web del programa de ingeniería de sistemas. Asimismo se plantean como objetivos generales el identificar las estrategias didácticas que promuevan el desarrollo de competencias labores específicas aplicables a la asignatura Ingeniería Web del Programa de Ingeniería de

Sistemas de la Corporación, y específicos, identificar las competencias laborales específicas que exige el mercado a los Ingenieros de Sistemas cuyo perfil ocupacional sea la Ingeniería Web, identificar los recursos didácticos que pueden ser aplicados en el desarrollo de la asignatura Ingeniería Web del Programa de Ingeniería de Sistemas de la Corporación e Identificar la relación entre el PEI, el programa de Ingeniería de Sistemas y asignatura Ingeniería Web. Dado el planteamiento de esta propuesta sobre Modelos prácticos y conceptuales de tipo didáctico que orienten estrategias a seguir en los procesos de enseñabilidad y aprendibilidad de la asignatura Ingeniería Web del Programa de Ingeniería de Sistemas de la Corporación y las competencias laborales específicas propias para profesionales con perfil ocupacional en Ingeniería Web, el mismo proporciona en este sentido aspectos que orientan la propuesta sobre estrategias de enseñanza-aprendizaje de la auditoria informática y por ende el desarrollo de las competencias profesionales.

Unda (2004), en su trabajo titulado "*Módulo Instruccional Introducción a la computación"*, tuvo como objetivo fundamental el diseño de un manual instruccional de carácter teórico practico para la comunidad estudiantil cursante de la materia Introducción a la Computación de la carrera de Ingeniería en Informática que dicta la Universidad Centroccidental " Lisandro Alvarado" de Barquisimeto, Estado Lara. La investigación es considerada de naturaleza documental ya que la misma se apoya en la búsqueda, revisión y análisis de diversas fuentes de información relacionados con el área y el diseño de recursos instruccionales. Además tomando como base lo investigado se concluye en que los módulos instruccionales se constituyen en una herramienta didáctica de alto valor académico, que facilita el acceso de la comunidad universitaria a diversidad de materiales que apoyan el desarrollo cognitivo del individuo, así como también se asientan en la base de ser un recurso actualizado y pertinente en cuanto a los avances y descubrimientos tecnológicos e informáticos se refiere.

Es por ello, que este trabajo proporcionó un gran apoyo teórico-práctico, para el desarrollo de la presente propuesta sobre Estrategias para el Proceso Enseñanza-Aprendizaje de la asignatura Auditoria Informática, correspondiente al pensum de la carrera Ingeniería en Informática del Decanato de Ciencias y Tecnología.

Ruiz y Castañeda (2004), en su trabajo "*La introducción de foros electrónicos asincrónicos para el perfeccionamiento de la función docente de los profesores desde concepciones de la gestión de la innovación tecnológica*", plantean que una comunidad virtual que se concibe y se implanta con la ayuda de las herramientas y concepciones de la Gestión de la Innovación Tecnológica puede transformar de forma significativa las habilidades de sus miembros y los procesos en que se inserta, asimismo dicen que las actividades docente metodológicas dirigidas al perfeccionamiento de la función docente de los profesores de una institución educativa puede ser uno de los procesos específicos transformado mediante la introducción de foros virtuales asincrónicos.

En el presente trabajo se aborda el perfeccionamiento de procesos y escenarios establecidos en instituciones de Educación Superior para el Trabajo Docente Metodológico de las comunidades de profesores universitarios mediante el empleo de foros virtuales asincrónicos, desde la perspectiva de la Gestión de la Innovación Tecnológica (GIT), como una expresión de la asimilación de las Tecnologías de la Información y las Comunicaciones (TIC) y la Gestión de la Información y el Conocimiento (GIC) en un proceso específico de estas instituciones. De ahí que uno de los campos de acción de la Gestión de la Innovación Tecnológica es el perfeccionamiento de procesos mediante la introducción de nuevas tecnologías, aspectos estos de interés al tema abordado en esta investigación, ya que la misma presenta elementos importantes que combinados con la tecnología, pueden contribuir con el perfeccionamiento docente y las estrategias del proceso de enseñanza-aprendizaje.

Bases Teóricas

Sistema de Información

Laudon y Laudon (2004), definen técnicamente un sistema de información como “un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización” (p.8), es decir un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio, por lo que interesa al mundo entero contar con eficientes y eficaces sistemas de información que faciliten los procesos que se siguen en las empresas, independiente del objeto al cual se dediquen. Se entiende por información los datos que han sido procesados y son de utilidad para la personas, a diferencia con los datos que son hecho en bruto sin procesar y representan eventos en un momento determinado y que no han sido ordenado de manera que sean entendibles.

En este sentido los avances vertiginosos que sufren constantemente las tecnologías y por ende los sistemas de información ameritan que se esté evaluando constantemente su funcionalidad a fin de dar respuestas rápidas y oportunas a los diferentes procesos de gestión que involucran.

Los mismos pueden clasificarse según lo planteado por Laudon y Laudon (2004), tomando en cuenta la información diferenciada, de acuerdo a los niveles organizacionales, en: Sistemas de Apoyo a Ejecutivos (ESS), Sistemas de información Gerencial (MIS), Sistemas de Apoyo a la Toma de Decisiones (DSS) Sistemas de Trabajo del Conocimiento (KWS), Sistemas de Oficina y Sistemas de Procesamiento de Transacciones (TPS).

a.- Sistema de Apoyo a Ejecutivos (ESS).

Los sistemas de apoyo a ejecutivos (ESS), afrontan la toma de decisiones no estructurada, es decir apoyan al nivel estratégico de la

organización en decisiones que no son de rutina, en las cuales necesariamente se requiere del juicio, evaluación y comprensión, utiliza herramientas como gráficos y medios de comunicación avanzada.

Sistemas a Nivel Estratégico				
Sistemas de apoyo a Ejecutivos (ESS)	Pronóstico de tendencia de ventas a cinco años	Plan Operativo a cinco años	Pronóstico de presupuesto para cinco años	Planeación de utilidades	Planeación de Personal

Figura 1. Sistemas de Apoyo a Ejecutivos (ESS).

Fuente: Laudon y Laudon (2004). Elaboración y complementación: Camacaro (2006).

b.- Sistema de Información Gerencial (MIS).

Según Laudon y Laudon (2004), "Los Sistemas de Información Gerencial (MIS), apoyan al nivel administrativo de la organización, proveyendo de informes a los gerentes y, en algunos casos, de acceso en línea al desempeño real y los registros históricos de la organización" (p.43), por tanto puede decirse que proporcionan herramientas a las funciones de planificación, control y toma de decisiones, proporcionando informes resumidos sobre la gestión realizada.

c.- Sistemas de Apoyo a la Toma de Decisiones (DSS)

El autor antes mencionado plantea en lo que respecta a los Sistemas de Apoyo a la Toma de decisiones (DDS), "que ayudan a los gerentes a tomar decisiones que son exclusivas, rápidamente cambiantes y no especificadas fácilmente con anticipación" (p.45), es decir abordan y apoyan el proceso de toma de decisiones semi-estructura y no estructura, combinando datos y modelos de análisis sofisticados, con herramientas de análisis de datos.

Estos sistemas se ubican en el nivel administrativo de la organización.

Sistemas a Nivel Administrativo

Sistemas de Información Gerencial (MS)	Administración de Ventas	Control de Inventarios	Elaboración de Presupuesto Anual	Análisis de Inversión de Capital	Análisis de reubicación
Sistemas de Apoyo a la Toma de Decisiones (DSS)	Análisis de la región de ventas	Programación de la producción	Análisis de costos	Análisis de fijación de precios y rentabilidad	Análisis de costo de contratos

Figura 2. Sistemas de información Gerencial (MIS) y Sistemas de Apoyo a la Toma de Decisiones (DSS).

Fuente: Laudon y Laudon (2004). Elaboración y complementación: Camacaro (2006).

d.- Sistemas de Trabajo del Conocimiento (KWS).

Los Sistemas de Trabajo del Conocimiento (KWS), apoyan a los trabajadores del conocimiento, en la creación e integración del conocimiento naciente en la organización, entendiendo esto según lo planteado por Laudon y Laudon (2004), que los trabajadores del conocimiento son personas con títulos universitarios y cuya actividad principal es crear información y conocimientos.

e.- Sistemas de Oficina.

Asimismo los sistemas de oficina, se refieren a procesadores de palabra, de correo electrónico y sistemas de programación, diseñados para aumentar la productividad de los datos en la oficina y que sirven de apoyo a los trabajadores de datos (procesan la información). Ambos sistemas se ubican en el Nivel de Conocimiento de la Organización.

Sistemas a Nivel del Conocimiento

Sistemas de trabajo del conocimiento (KWS)	Estaciones de trabajo para ingeniería	Estaciones de trabajo para gráficos	Estaciones de trabajo para gerentes
Sistemas de Oficina	Procesamiento de textos	Digitalización de documentos	Calendarios Electrónicos

Figura 3. Sistemas de Trabajo del Conocimiento (KWS) y Sistemas de Oficina.

Fuente: Laudon y Laudon (2004). Elaboración y complementación: Camacaro (2006).

f.- Sistemas de Procesamiento de Transacciones (TPS).

Estos Sistemas de Procesamiento de Transacciones (TPS), son aquellos que registran las operaciones u transacciones diarias necesarias para la dirección del negocio y se ubican en el nivel operativo de la organización, por ejemplo entradas de las ventas, nómina etc.

Sistemas a Nivel Operativo

Sistemas de Procesamiento de transacciones (TPS)	Seguimiento de pedidos	Control de Máquinas Programación de Planta	Negociación de Valores	Nómina de Cuentas por Pagar	Compensaciones Capacitación y Desarrollo
	Procesamiento de pedidos	Control de movimiento de materiales	Administración del efectivo	Cuentas por cobrar	Registro de empleados
	Ventas y marketing	**Manufactura**	**Finanzas**	**Contabilidad**	**Recursos Humanos**

Figura 4. Sistemas de Procesamiento de Transacciones (TPS).

Fuente: Laudon y Laudon (2004). Elaboración y complementación: Camacaro (2006).

Otra clasificación de los sistemas de información es la siguiente:

1. Sistemas de información Transaccionales

Sus principales características son:

1.1. Automatizan tareas operativas de la Organización.

1.2. Apoyan las tareas a nivel operativo de la Organización.

1.3. Desarrollan procesos simples y pocos complejos.

1.4. Manejadores de grandes bases de datos.

1.5. Proporcionar grandes benéficos a la organización.

2. Sistemas de información de Apoyo a las Decisiones.

Estos sistemas pueden definirse como, como un conjunto de programas y herramientas que permiten obtener de manera oportuna la información que se requiere mediante el proceso de la toma de decisiones que se desarrolla en un ambiente de incertidumbre. Ayudan a la toma de decisiones de los administradores al combinar datos, modelos analíticos sofisticados y software amigable en un solo sistema poderoso que puede dar soporte a la toma de decisiones semiestructuradas o no estructuradas. El DSS esta bajo el control del usuario desde la concepción inicial a la implantación final y uso diario.

3. Sistemas de información Estratégicos.

Puede decirse, según Casas (2005) “que estos sistemas apoyan directamente a las organizaciones, en sus planes, estrategias y acciones para lograr ventajas competitivas en un mercado globalizado”, lo indica que por ser estratégicos proyectas a la organización hacia fuera, proporcionándole innovación al negocio lo cual redunda en la calidad de los servicios que prestan.

Como puede observarse dada la diversidad de los sistemas de información, es competencia de la Auditora Informática ser herramienta de evaluación del funcionamiento de los mismos, de acuerdo a los niveles de ubicación y necesidades de información en

la organización, además el auditor informático debe entrevistar a individuos claves que usan y operan un sistema de información específico, para evaluar actividades y procedimientos de los mismos. Conviene revisar en este sentido las particularidades de la Auditoria Informática.

Auditoría Informática

Tradicionalmente se conoce a la Auditoría como el examen crítico que realiza el Licenciado en Contaduría o contador independiente, de los libros, registros, recursos, obligaciones, patrimonio y resultados de una entidad, basados en principios de contabilidad, normas, técnicas y procedimientos específicos con la finalidad de opinar sobre la razonabilidad de la información financiera.

Es un examen crítico, que se realiza con objeto de evaluar la eficiencia y la eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.

La palabra auditoría proviene del latín *auditorius***,** y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

La auditoría de sistemas es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación de los sistemas de información en la empresa [Rivas, 1988].

La auditoría de sistemas es fundamental para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos.

Según ISACA (2002), los auditores de sistemas de información examinan y evalúan el desarrollo, implementación, mantenimiento y operación de los componentes de sistemas automatizados y sus interfaces con sistemas externos y no automatizados.

Evolución de la Auditoría.

La Auditoría ha estado en constante evolución para tratar de garantizar la fiabilidad de la información económica-financiera demandada socialmente.

En un principio la función de la Auditoría se limitaba solo a la vigilancia con el fin de evitar errores y fraudes.

A principios de la revolución industrial, no hay grandes transacciones, la misión del auditor era buscar si se había cometido fraude en los negocios existentes, estos negocios eran pequeños.

Al Reino Unido se le Atribuye el origen de la Auditoría, entendida en términos de hoy en día. En la actualidad se puede decir que los E.E.U.U. son los pioneros y más vanguardistas (fue impulsado por el crack de 1929 en wall street). En 1988 se aprobó la Ley de Auditoría de cuentas (LAC).

1. Fundamentos de la Auditoría.

   1.1. 1917: Se forma la Primera agrupación profesional, la cual fue denominada Asociación de Contadores Públicos contando con 11 miembros.

   1.2. 6 de Octubre de 1923: Se constituyó el Instituto de Contadores Públicos titulados de México, cuya finalidad era agrupar a los miembros de la profesión. Con el crecimiento de la profesión y el nacimiento de la Ley General de Profesiones originaron el nacimiento de agrupaciones regionales de contadores.

   1.3. 1965: El Instituto Mexicano de Contadores Públicos adquirió el carácter de organismo nacional con el propósito de representar a la población contable nacional.

   1.4. 1977: Obtiene el reconocimiento oficial de Federación de Colegios de Profesionistas.

   1.5. 30 de Octubre de 1987: Estatutos y reglamentos del IMCP.

Las empresas comienzan a crecer y se hacen más grandes, se separa el capital y la propiedad del negocio, es decir, nace la Administración y con ella una función formal para la Auditoría como es la de verificar, certificar, que la información reflejada por los administradores en la cuenta de resultados, sea veraz.

Hoy en día, la auditoria determina la veracidad de los estados financieros de las empresas, en cuanto a la situación patrimonial y los resultados de sus operaciones.

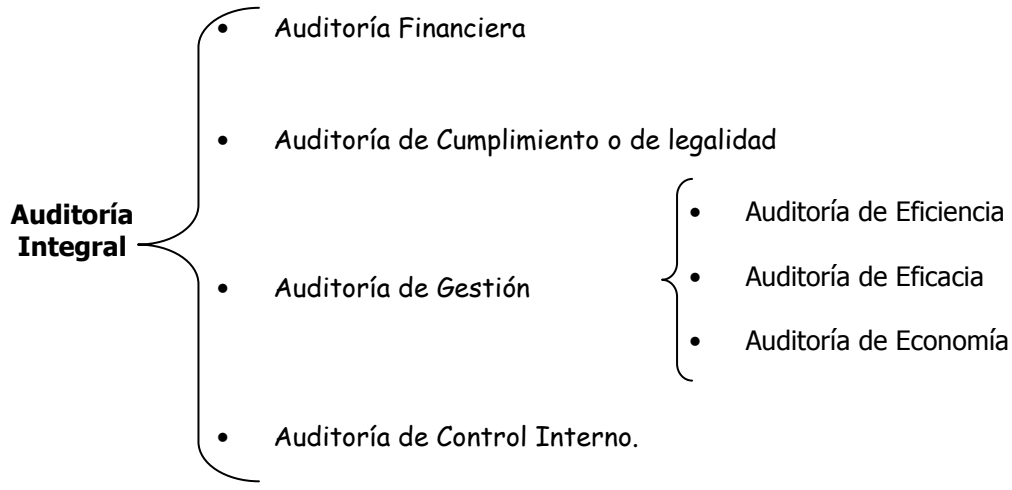
2. Tipos de Auditoría:

Tradicionalmente se reconocen 2 clases: auditoría interna y auditoría externa. Tomando como base la fecha en que son aplicadas las auditorías externas, éstas se clasifican en:

2.1. Auditoría detallada.

2.2. Auditoría preliminar.

2.3. Auditoría final.

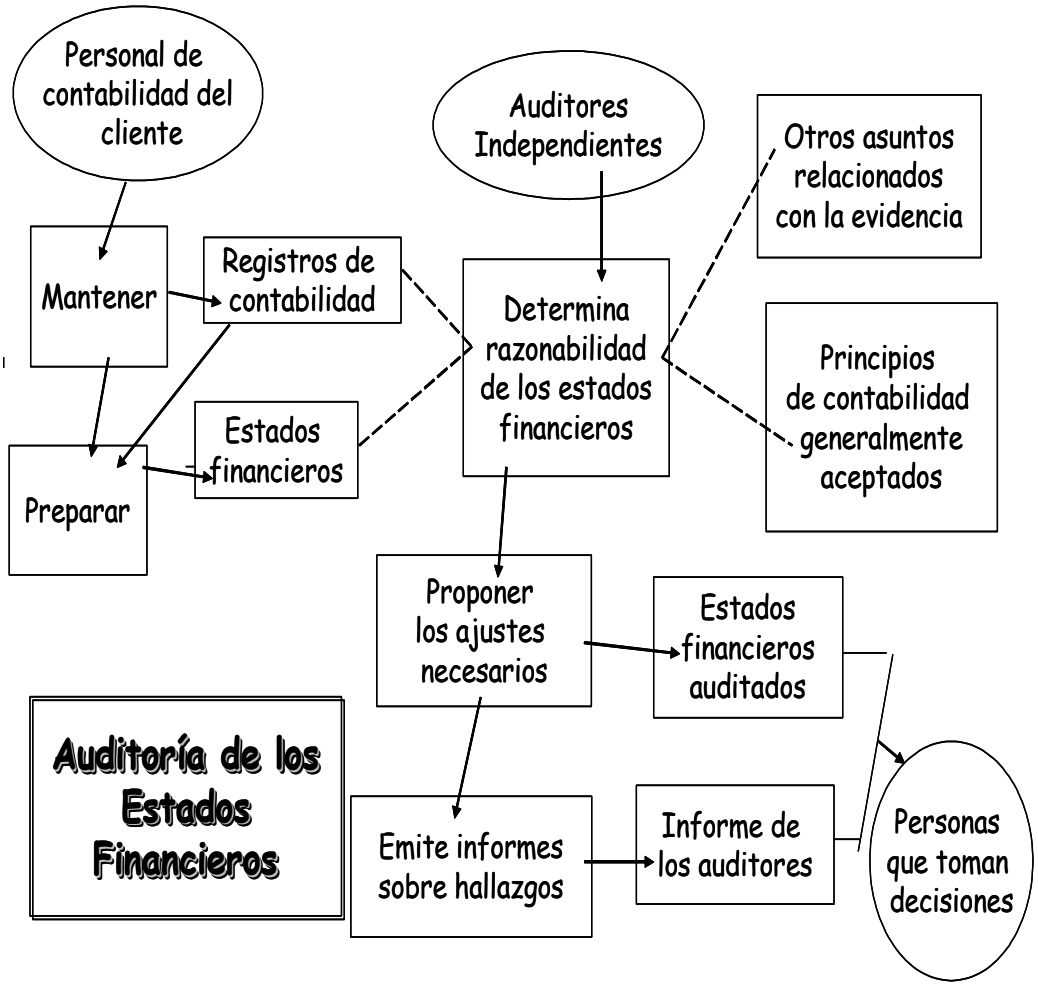


Además existen auditorías tales como:

- Auditorías de Estados Financieros.
- Auditorías Operacionales
- Auditorías de Cumplimiento.
- Auditoría de Actuación.
- Auditoría de Programa.

- Auditoría Operacional.
- Auditoría Administrativa.
- Auditoría Operativa.
- Auditoría de Sistemas.
- Auditoría de Calidad.
- Auditoría de Performance (Desempeño).

3. Auditoría de los Estados Financieros.



IMPORTANCIA DE LA AUDITORÍA EN EL DISEÑO DE ESTRATEGIAS PARA LA EVALUACIÓN DE LOS SISTEMAS DE INFORMACIÓN.

Independientemente del tipo de Organización y de actividad que se realice, la Auditoría constituye una herramienta de gran importancia toda vez que proporciona a la organización que se evalué adecuadamente por ejemplo: el control de la función informática, el análisis de la eficiencia de los Sistemas Información, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

Normas de Auditoría.

Las normas de auditoría, son un conjunto de principios que se refieren, no sólo a las cualidades personales del auditor, sino también al ejercicio de su juicio en el desarrollo de su examen y a la información relativa a él. Las normas no varían.

1. Origen

   Las normas de auditoría surgen con la finalidad de asegurar que el desempeño del auditor se efectué a un nivel alto de calidad.

2. Normas de Auditoria actualmente existentes

   2.1. Las Normas y Procedimientos de Auditoría nacionales promulgadas por la Federación de Colegios de Contadores Públicos de Venezuela (FCCPV).

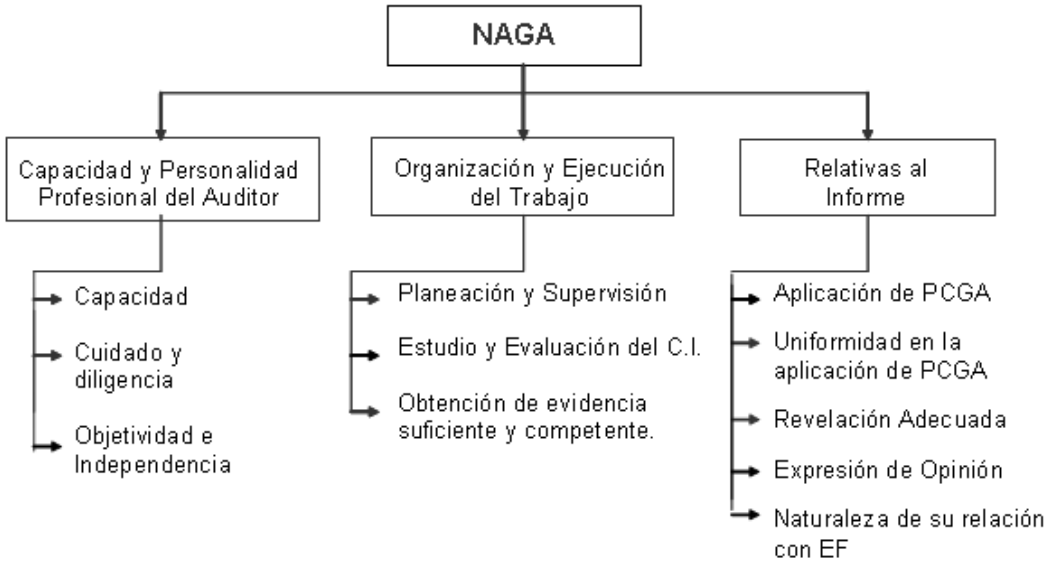
   2.2. Las Normas y Procedimientos de Auditoría Internacionales promulgadas por el Comité Internacional de Prácticas de Auditoría (IAPC), adscrito a la Federación Internacional de Contadores (IFAC)

   2.3. Normas y Procedimientos de auditoria del Instituto Mexicano de Contadores Públicos (IMCP)

   2.4. Normas de Auditoria Gubernamental del Perú.

Órganos Competentes para la emisión de normas en Venezuela

En Venezuela tiene la atribución la Federación de Colegios de Contadores Públicos de Venezuela (FCCPV). En la publicación técnica No. 1 (PT1), se encuentran las Normas de Auditoría de aceptación general, vigentes desde septiembre de 1974. Las Normas de Auditoria Generalmente Aceptadas son las siguientes:



Declaración de Normas y Procedimientos de Auditoría:

- (DNA 1) Papeles de trabajo.
- (DNA 2) Solicitud de información al abogado del cliente.
- (DNA 3) Manifestaciones de la Gerencia.
- (DNA 4) El Informe de Control Interno.
- (DNA 5) Efecto de la Función de auditoria en el alcance del examen del Contador.

Público Independiente (CPI)

- (DNA 6) Planificación y Supervisión.
- (DNA 7) Transacciones entre partes relacionadas.
- (DNA 8) Comunicación entre el auditor predecesor y sucesor.
- (DNA 9) Procedimientos analíticos de revisión.
- (DNA 10) Evidencia Comprobatoria.

- (DNA 11) El Dictamen del C.P.I. sobre los Estados Financieros (E.F.).
- (DNA 12) El Dictamen del C.P.I. sobre los E.F.
- (DNA 13) Control Calidad en el Ejercicio Profesional.
- (DNA 14) El Examen de la Información Técnica Prospectiva

Normas Internacionales de Auditoría:

El objetivo fundamental es contribuir al desarrollo y realce de la profesión contable mundial coordinada y con normas armonizadas.

Las Normas Internacionales de Auditoria pretenden su aceptación y aplicación mundial; sin embargo no prevalecen sobre las reglamentaciones locales que rigen la auditoria de información financiera de cada país. En la medida que estas normas estén de acuerdo con las reglamentaciones locales sobre un asunto en particular, la auditoria de información financiera en dicho país estará realizada de acuerdo con dichas reglamentaciones y cumplirá automáticamente con las normas internacionales relativas a esa materia.

Cuando la reglamentación o normativa de Venezuela no contemple algún asunto contenido en las normas internacionales es recomendable que se utilicen de manera supletoria. Al respecto la FCCPV, en el párrafo 47 de las DPC-0 normas básicas y principios de contabilidad de aceptación general establece como se deben aplicar de manera supletoria otros pronunciamientos.

Aunque estos criterios están referidos a los principios de contabilidad, consideramos que por analogía, para las normas de auditoria debe aplicarse la misma metodología.

De acuerdo a ese orden los organismos autorizados para emitir normas de auditoria son:

- Venezuela

  Federación de Colegios de Contadores Públicos

  Declaración de Normas de Auditoria (DNA)

- Internacionales

Federación Internacional de Contadores

Normas Internacionales de Auditoria (NIAS)

- México

Instituto Mexicano de Contadores Públicos

Boletín de Normas de Auditoria

- Estados Unidos

Instituto Americano de Contadores Públicos (SAS)

Normas de Auditoría Informática.

-Emitidas por ISACA, organismo fundado en Chile en 1969.

-ISACA auspicia conferencias nacionales e internacionales, administra globalmente la rendición de los exámenes de certificación mundial CISA *(Certified Information Systems Auditor)* y CISM *(Certified Information Security Manager)* y desarrolla globalmente Estándares de Auditoria y Control en Sistemas de Información.

Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información. Estas Normas sirven de referencia para los trabajos de Auditoría Informática.

Objetivos

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

NORMAS GENERALES PARA LOS SISTEMAS DE AUDITORÍA DE LA INFORMACIÓN

Según ISACA (1997), son:

010 Título de auditoria

010.010 Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

020 Independencia

020.010 Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

020.020 Relación organizativa

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

030 Ética y normas profesionales

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.

040 Idoneidad

040.010 Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

040.020 Educación profesional continúa

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

050 Planificación

050.010 Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

060 Ejecución del trabajo de auditoría

060.010 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

060.020 Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

070 Informes

070.010 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

080 Actividades de seguimiento

080.010 Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Entraron en vigencia el 25 de julio de 1997

Por otra parte ISACA plantea que la estructura para los Estándares de Auditoría de Sistemas de Información (SI), brinda múltiples niveles de asesoramiento:

- Los Estándares definen requisitos obligatorios para la auditoría y el reporte de SI. Informan a:
  - Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el Código de Ética Profesional de ISACA.

- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de Auditor Certificado de Sistemas de Información (Certified Information Systems Auditor®, CISA®) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la Junta de Directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias.

- Las Directrices proporcionan asesoramiento en la aplicación de los Estándares de Auditoría de SI. El auditor de SI debe considerarlas al determinar cómo lograr la implementación de los estándares, utilizar un buen juicio profesional en su aplicación y estar dispuesto a justificar cualquier desviación de las mismas. El objetivo de las Directrices de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.
- Los Procedimientos proporcionan ejemplos de procedimientos que podría seguir un auditor de SI en el curso de un contrato de auditoría. Los documentos sobre procedimientos proporcionan información sobre cómo cumplir con los estándares al realizar trabajos de auditoría de SI, pero no establecen los requisitos correspondientes. El objetivo de los Procedimientos de Auditoría de SI es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

CONTROL INTERNO INFORMÁTICO.

Constituye un conjunto de reglas, lineamientos, actividades a seguir, que controlan el funcionamiento de los sistemas de información, de acuerdo a procedimientos e indicadores previamente establecidos. El

mismo puede ser manual o automatizado. Sus principales áreas de interés son:

1. Objetivos.

Asegurarse del cumplimiento de los procedimientos, normas y/o leyes.

Apoyar el trabajo de auditoria Informática, tanto interna como externa.

Medir el grado de eficacia y eficiencia de los servicios que se prestan en materia de informática.

Proporcionar apoyo y asesorías al Departamento de Ingeniería Informática.

2. Tipos de Controles.

En el ambiente informático, el control interno se materializa fundamentalmente en controles de dos tipos:

2.1. Controles manuales; aquellos que son ejecutados por el personal del área usuaria o de informática sin la utilización de herramientas computacionales.

2.2. Controles Automáticos; son generalmente los incorporados en el software, llámense estos de operación, de comunicación, de gestión de base de datos, programas de aplicación, etc.

Los controles de acuerdo a su finalidad se clasifican en: (Según Piattini y otros (2004) Auditoria Informática).

- Controles Preventivos: Trata de evitar que los hechos ocurran, como un software de seguridad que impida los accesos no autorizados al sistema

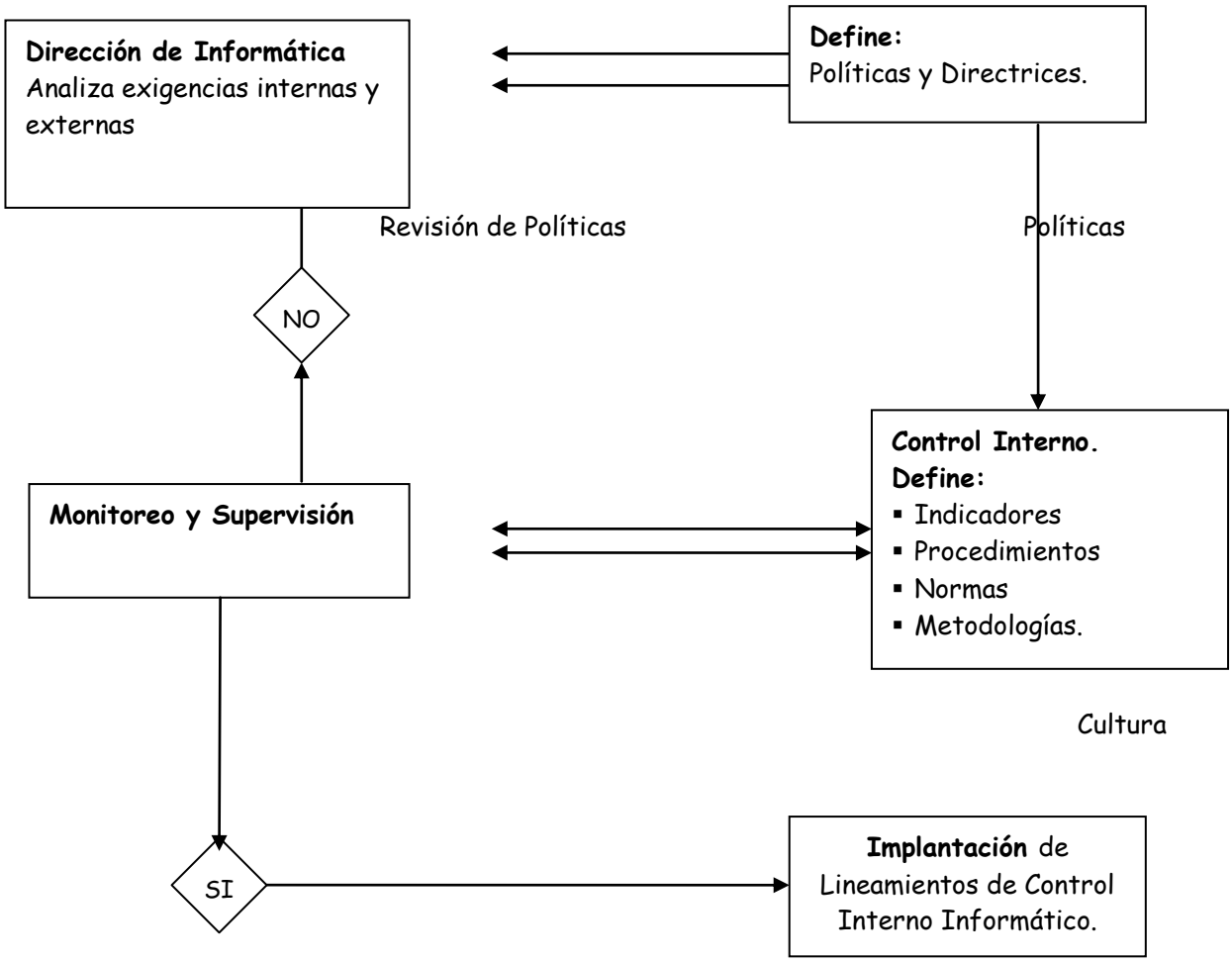
- Controles Detectivos: Fallan los preventivos para tratar de conocer cuanto antes los eventos. Por Ejemplo, el registro de accesos no autorizados, el registro de la actividad diaria para detectar errores u omisiones etc.

- Controles Correctivos: Facilitan que todo vuelva a la normalidad cuando se han producido incidencias. Por Ej. La recuperación de un archivo dañado a partir de las copias de seguridad.

¿Qué se debe controlar?

El entorno de red, configuración del computador base, entorno de aplicaciones, productos y herramientas, la seguridad entre otros.

Implantación del Control Interno Informático.



Metodologías de Control Interno Informático.

Regulación internacional sobre Auditoría de Sistemas de Información. En materia de Auditoría de Sistemas de Información existen varias metodologías desde el enfoque de control a nivel internacional. Algunas de las más importantes para los profesionales de la contabilidad y la auditoría son:

- ISACA(COBIT) = Asociación de Auditoría y Control de Sistemas de Información (Objetivos de Control para la Información y Tecnologías Afines).
- COSO = Organizaciones que patrocinan la Comisión de Treadway
- AICPA (SAS) = Instituto Americano de contadores Públicos (Normas de Financieras de Auditoria).
- IFAC (NIA) = La Federación Internacional de Contables (Normas Internacionales de Auditoria).
- SAC = Sistemas de Auditoria y Control.
- MARGERIT = (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).
- EDP = Es una Fundación de Auditores.

COSO

"Informe COSO", que se denomina "control interno - Un marco general integrado" (Internal Control-Integrated Framework) que fue emitido por el "Committee of Sponsoring Organizations of the Treadway Commission" (COSO), en la que participan organizaciones tan prestigiosas y conocidas como el American Institute of Certified Public Accountants(AICPA), la American Accounting Association, el Institute of Internal Auditor, el Institute of Management Accountants y el Financial Executive Institute, que encargó la redacción del Informe a Coopers & Lybrand.

El informe COSO nos da una definición integradora de control interno con el objetivo de facilitar un modelo en base al cual las empresas y otras entidades puedan evaluar sus sistemas de control y decidir cómo mejorarlos, sus ámbitos o categorías son las siguientes:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

Todo esto queda reflejado en la siguiente gráfica.

Indicadores

Fuente: INTOSAI (2001). Guía para las normas de control interno del sector público

COBIT

ISACA, propone la metodología COBIT (Control Objectives for Information and related Technology). Es un documento realizado en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones.

Es un sistema de control interno en Tecnología Informática, ésta diseñado como un amplio "checklist" para los propietarios del proceso del negocio y de gran ayuda para los usuarios y los Auditores.

La Estructura COBIT provee una herramienta para el propietario del proceso del negocio que facilita el descargo de su responsabilidad. La estructura comienza con una premisa simple y pragmática:

Los Recursos de Tecnología Informática necesitan ser administrados por un conjunto de procesos de Tecnología Informática

agrupados naturalmente para proveer la información que necesita la empresa para el logro de sus objetivos.

Posee un conjunto de 34 Objetivos de Control de alto nivel, uno por cada uno de los Procesos de Tecnología Informática, agrupados en cuatro Dominios:

- Planeamiento y Organización
  - Po1. Definición de un plan estratégico
  - Po2. Definición de la arquitectura de información
  - Po3. Determinación de la dirección tecnológica
  - Po4. Definición de organización y relaciones
  - Po5. Administración de la inversión
  - Po6. Comunicación de las políticas
  - Po7. Administración de los recursos humanos
  - Po8. Asegurar el cumplimiento con los requerimientos Externos
  - Po9. Evaluación de riesgos
  - Po10. Administración de proyectos
  - Po11. Administración de la calidad

- Adquisición e Implementación
  - A11. Identificación de soluciones automatizadas
  - A12. Adquisición y mantenimiento del software aplicativo
  - A13. Adquisición y mantenimiento de la infraestructura tecnológica
  - A14. Desarrollo y mantenimiento de procedimientos
  - A15. Instalación y aceptación de los sistemas
  - A16. Administración de los cambios

- Entrega y Soporte
  - Ds1. Definición de los niveles de servicios
  - Ds2. Administrar los servicios de terceros
  - Ds3. Administrar la capacidad y rendimientos
  - Ds4. Asegurar el servicio continuo
  - Ds5. Asegurar la seguridad de los sistemas

Ds6. Entrenamiento a los usuarios

Ds7. Identificar y asignar los costos

Ds8. Asistencia y soporte a los clientes

Ds9. Administración de la configuración

Ds10. Administración de los problemas

Ds11. Administración de los datos

Ds12. Administración de las instalaciones

Ds13. Administración de la operación

- Monitoreo

  M1. Monitoreo del cumplimiento de los objetivos de los procesos de tecnología de la información.

  M2. Evaluar lo adecuado del control interno

  M3. Obtener aseguramiento independiente

  M4. Proporcionar auditoría independiente

En la Estructura COBIT se destaca el impacto sobre los recursos de Tecnología Informática junto con los requerimientos del negocio que necesitan ser satisfechos, en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Adicionalmente, la Estructura brinda definiciones para los requerimientos del negocio que son destilados de niveles más altos de objetivos para calidad, seguridad e información financiera según se relacionan con Tecnología Informática.

Guías de Auditoría

Las guías de Auditoría se distribuyen entre los 34 Subdominios y su objetivo es poder realizar una revisión de tercer nivel en la práctica de la Gestión de Tecnología.

COBIT como herramienta de Evaluación o Auditoría se fundamenta en la estructura antes mencionada 4 Dominios, 34 Subdominios, 318 Objetivos de Control y 376 Guías de Auditoría, con esta combinación se

puede realizar una evaluación completa de las prácticas en el área de tecnología.

- IFAC (NIA): La Federación Internacional de Contables IFAC (http://www.ifac.org) emitió las Normas Internacionales de Auditoría NIA 15, 16 y 20 en 1991. IFAC muestra en la NIA 15 (Auditoría en Entornos Informatizados) una referencia de controles para procesamiento electrónico de datos y la necesidad de estos cuando estamos en ambientes donde los instrumentos tradicionales del papel y demás pistas de auditoría no son visibles para los contables en el momento de realizar su trabajo.

  La NIA 16 (Técnicas de Auditoría Asistida por Computador) describe técnicas y procedimientos de auditoría que se pueden hacer en entornos informatizados con ayuda de los computadores y otras tecnologías.

  La NIA 20 nos presenta los efectos de un entorno informatizado en la evaluación de sistemas de información contables. Junto con las demás normas dan una guía al auditor de los controles en general a tener en cuenta en un ambiente informatizado y en las aplicaciones que procesan la información, así como técnicas de auditoría asistidas por computador y su importancia.
- SAC: Realizado en 1991 y revisado posteriormente. Ofrece una guía de estándares y controles para los auditores internos en el área de auditoría de sistemas de información y tecnología. Tiene como objetivos de control la efectividad y eficiencia de las operaciones, la integridad de la información financiera y el cumplimiento de normas y regulaciones que explica en el ambiente de control, sistemas manuales y automatizados y procedimientos de control.
- MARGERIT: Consejo superior de informática del ministerio de administraciones públicas de España MARGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) 1997.

Es una metodología de análisis y gestión de riesgos de los sistemas de información de las administraciones públicas, emitida en el año 1997 por el consejo superior de informática y recoge las recomendaciones de las directivas de la Unión Europea en materia de seguridad de sistemas de información, esta metodología presenta un objetivo definido en el estudio de los riesgos que afectan los sistemas de información y el entorno de ellos haciendo unas recomendaciones de las medidas apropiadas que deberían adoptarse para conocer, prevenir, evaluar y controlar los riesgos investigados. Margerit desarrolla el concepto de control de riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de normas legales.

- EDP:

  La E.D.P. Auditors Foundation (EDPAF) fundada en 1976, es otra entidad de carácter educativo e investigativo en los temas sobre estándares para la auditoría de los sistemas de información.

  Esta fundación ha investigado sobre controles en los sistemas de información, generando los diez estándares generales de auditoría de sistemas y el código de ética para los auditores.

- ISACA

  Código de Ética Profesional de ISACA

  ISACA establece este Código de Ética Profesional para guiar la conducta profesional y personal de los miembros y/o poseedores de certificaciones de la asociación.

  Los miembros y los poseedores de certificaciones de ISACA deberán:

  - Respaldar la implementación y promover el cumplimiento con estándares y procedimientos apropiados del gobierno y gestión efectiva de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de auditoría, control, seguridad y riesgos.

- Llevar a cabo sus labores con objetividad, debida diligencia y rigor/cuidado profesional, de acuerdo con estándares de la profesión.
- Servir en beneficio de las partes interesadas de un modo legal y honesto y, al mismo tiempo, mantener altos niveles de conducta y carácter, y no involucrarse en actos que desacrediten a la profesión o a la Asociación
- Mantener la privacidad y confidencialidad de la información obtenida en el curso de sus deberes a menos que la divulgación sea requerida por una autoridad legal. Dicha información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.
- Mantener la aptitud en sus respectivos campos y asumir sólo aquellas actividades que razonablemente esperen completar con las habilidades, conocimiento y competencias necesarias
- Informar los resultados del trabajo realizado a las partes apropiadas, revelando todos los hechos significativos sobre los cuales tengan conocimiento
- Respaldar la educación profesional de las partes interesadas para que tengan una mejor comprensión del gobierno y la gestión de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de la auditoría, control, seguridad y riesgos.

El incumplimiento de este Código de Ética Profesional puede acarrear una investigación de la conducta de un miembro y/o titular de la certificación y, en última instancia, medidas disciplinarias.

Otras Normas Internacionales de Apoyo para la realización de Auditoría Informática

Existe a nivel internacional una serie de legislaciones en materia informática, y que de alguna manera regulan esta práctica, con la existencia de organismos tales como ISACA, el cual cuenta con – más de

95,000 miembros en todo el mundo – se caracterizan por su diversidad. Los miembros viven y trabajan en más de 160 países y cubren una variedad de puestos profesionales relacionados con TI – sólo por nombrar algunos ejemplos, auditor de SI, consultor, profesional de la educación, profesional de seguridad de SI, regulador, director ejecutivo de información y auditor interno. Algunos son nuevos en el campo, otros están en niveles medios de la gerencia y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, firmas de auditoría y consultoría, gobierno y sector público, servicios públicos y manufactura. Esta diversidad permite que los miembros aprendan unos de otros, e intercambien puntos de vista comunes sobre una variedad de tópicos profesionales. Esta ha sido considerada durante mucho tiempo como una de las fortalezas de ISACA. Previamente conocida como la Asociación de Auditoría y Control de Sistemas de la Información, ISACA ahora identificada ya por su acrónimo, para reflejar el amplio rango de profesionales del gobierno de las TI a los que sirve.

ISACA además ofrece cuatro certificaciones. La certificación *Certified Information Systems Auditor* "Auditor Certificado de Sistemas de Información", (CISA) es reconocida de forma global y ha sido obtenida por más de 75,000 profesionales desde su creación. La certificación *Certified Information Security Manager* "Gerente Certificado de Seguridad de Información", (CISM) se concentra exclusivamente en el sector de gerencia de seguridad de la información y ha sido obtenida por mas de 13,000 profesionales. La certificación *Certified in the Governance of Enterprise IT* "Certificado en Gobierno de TI de la Empresa" (CGEIT) promueve el avance de profesionales que desean ser reconocidos por su experiencia y conocimiento relacionados con el Gobierno de las TI y ha sido obtenida por mas de 4,000 profesionales. La nueva certificación *Certified in Risk and Information Systems Control* "Certificado en Riesgos y Controles de los Sistemas de Información" (CRISC) es para

profesionales de TI que identifican y gestionan los riesgos a través del desarrollo, implementación y mantenimiento de controles de SI.

Así mismo ofrece en materia de legislación el Código de Ética Profesional de ISACA, Estándares (normas) de ISACA para la auditoría de SI, Guías (directrices) de ISACA para la Auditoría de SI y Procedimientos de ISACA para la Auditoría de SI. A este respecto los Objetivos de los estándares de ISACA para la Auditoría de SI son;

– Informar a la gerencia y a otras partes interesadas sobre lo que pueden esperar profesionalmente de los trabajos de auditoría

– Informar a los auditores de SI sobre el nivel mínimo de desempeño aceptable requerido para cumplir las responsabilidades profesionales establecidas en el Código de Ética Profesional de ISACA

La Estructura de los estándares de Auditoría de SI de ISACA es: Estándares, Guías y Procedimientos.

Los Estándares y guías de ISACA para la Auditoría de Sistemas comprenden:

– Estatutos de Auditoría
  - Responsabilidad, autoridad y sujeción a rendición de cuentas

– Independencia
  - Independencia profesional
  - Relación organizacional

– Ética Profesional y estándares
  - Código de Ética profesional
  - Debido cuidado profesional

– Competencia
  - Habilidades y conocimiento
  - Educación profesional continua

– Planeación
  - Planeación de la Auditoría

– Ejecución del trabajo de auditoría
  - Supervisión
  - Evidencia

– Reportes
  - Contenido y forma del reporte

– Actividades de seguimiento
  - Revisar conclusiones y recomendaciones anteriores
  - Revisar hallazgos previos relevantes
  - Determinar si han sido implementadas oportunamente acciones apropiadas

Utilización de las Guías de ISACA

– Considerar las guías en la determinación de cómo implementar los estándares

– Hacer uso del juicio profesional al aplicar estas guías

– Ser capaz de justificar cualquier desviación

Utilización de los Procedimientos de ISACA

– Ejemplos provistos para los procedimientos desarrollados por el Consejo de Estándares de ISACA.

– El auditor de SI debe aplicar su propio juicio profesional a las circunstancias específicas.

ISO

La Organización Internacional para la Estandarización, ISO por sus siglas en inglés (*International Organization for Standarization*), es una federación mundial que agrupa a representantes de cada uno de los organismos nacionales de estandarización y que tiene como objeto desarrollar estándares internacionales que faciliten el comercio internacional.

Los miembros de ISO, son organismos nacionales que participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (*International Electrotechnical Commission*), la organización que a nivel mundial prepara y publica estándares en el campo de la

electrotecnología. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (*Join Technical Committee Nº1*).

Los borradores de estas Normas Internacionales son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

La serie de normas que sirven de apoyo a la auditoria informática, varían de acuerdo al tipo de auditora a realizar:

ISO 27000

La serie ISO 27000 comprende un conjunto de normas relacionadas con la seguridad de la información y permite a las compañías certificar ISO y apoyan a las Auditorias Informática de Seguridad de la Información.

La familia de las normas ISO

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Muchos de ellos no están aún publicados, pero la estructura ya está definida:

- ISO/IEC 27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.
- UNE-ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005), publicada en el año 2007. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con

arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen.

- ISO/IEC 27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, publicada en el año 2005. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- ISO/IEC 27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases
- ISO 27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.
- ISO/IEC 27005:2008 Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.
- ISO/IEC27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información. Publicada en el año 2007. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios.
- ISO/IEC 27007. Guía para la realización de las auditorías de un SGSI.
- ISO/IEC 27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002. Contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la Norma ISO27001 y conseguir un nivel de seguridad aceptable.
- EN ISO 27799. Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC27002 (ISO27799:2008),

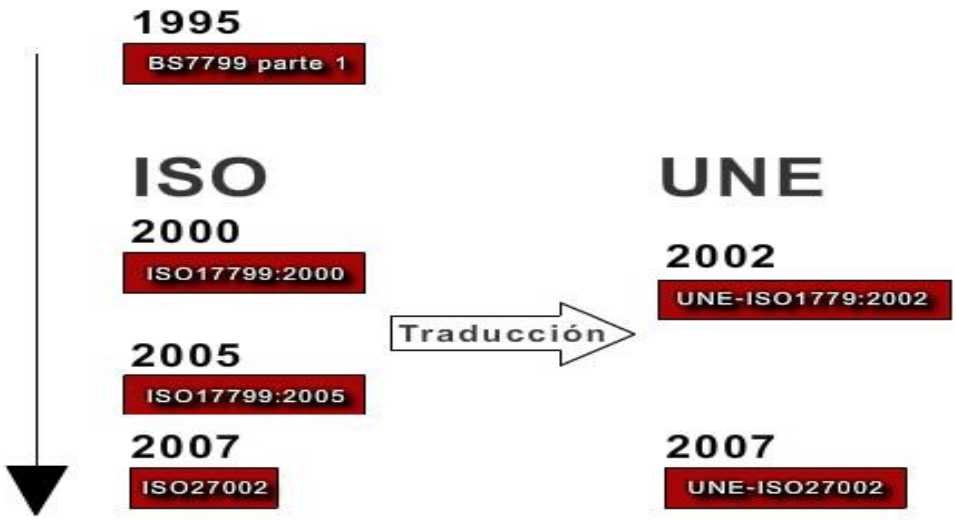
ha sido ratificada por AENOR (ESPAÑA) en agosto de 2008. Como en la anterior, es una guía sectorial que da cabida a los requisitos específicos de entorno sanitario.

Adopción de la Normas ISO por parte de España

La Norma ISO 27001

Orígenes

La Norma fue publicada como Norma Española en el año 2007, pero tiene una larga historia antes de llegar a este punto. Ya en el año 1995 el British Standard Institute (BSI) publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.



A la vista de la gran aceptación de esta Norma, en 1998, el BSI pública la norma BS7799-2, Especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2001. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799.

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2, sin que haya un equivalente ISO.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27002 y en octubre de 2007 la norma ISO 27001 se adopta como UNE. Con la publicación de la UNE-ISO/IEC 27001, dejó de estar vigente la UNE 71502 y las empresas nacionales se certifican ahora únicamente con esta nueva norma (UNE-ISO/IEC 27001).

Contenido de la UNE-ISO/IEC 27001

La norma UNE-ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización.

Como otras Normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

Asimismo está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La Norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua.

La Norma recoge:

- Los componentes del SGSI, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y

mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.

- Cómo se debe diseñar e implantar el SGSI.
- Define los controles de seguridad a considerar. Se requiere que se escojan los controles del Anexo A, que recoge todos los controles detallados en la Norma ISO/IEC 27002.
- Cómo debe realizarse la revisión y mejora del SGSI.

La ISO 27001 adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización.

La Norma ISO 27002

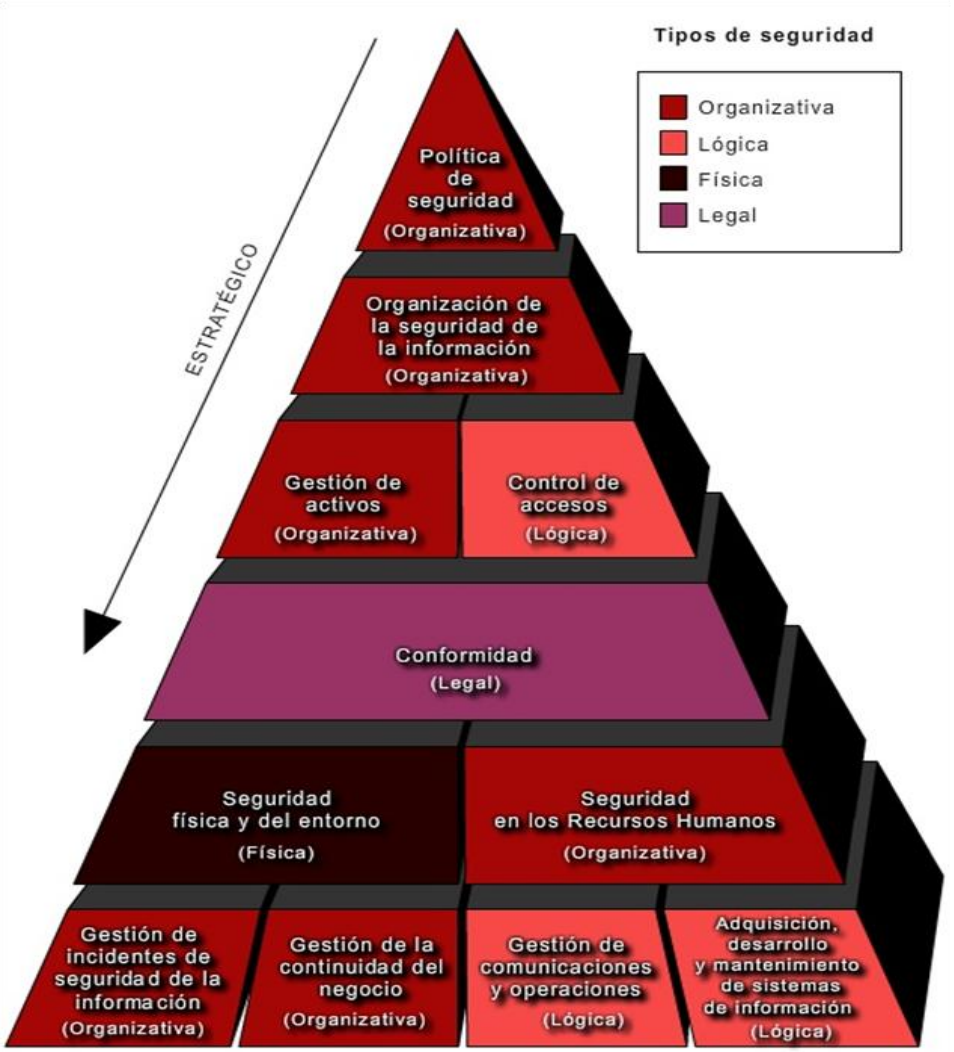
Esta norma contiene 11 capítulos de controles de seguridad que contienen un total de 133 controles de seguridad. Puede servir de guía práctica para la gestión de la seguridad de la información. No es una norma certificable.

Los objetivos de control contemplados en la Norma son:

- Política de seguridad. Cuenta con dos controles: Documento de Política de seguridad y Revisión del Sistema.
- Organización de la seguridad de la información, tienen 11 controles: Compromiso de la Dirección, Identificación de riesgos relacionados con terceras partes.
- Gestión de activos, con 5 controles: Utilización aceptable de los activos, etiquetado y tratamiento de la Información
- Seguridad ligada a los Recursos Humanos con 9 controles: Análisis y selección, Retirada de los derechos de acceso.
- Seguridad física y del entorno tiene 13 controles: Controles físicos de entrada, emplazamiento y protección de los equipos.
- Gestión de comunicaciones y operaciones, con 32 controles es el capítulo más extenso y más técnico: Gestión de la Capacidad,

Protección frente a código malicioso, Copias de seguridad, Registro de fallos

- Control de acceso, cuenta con 25 controles: Gestión de contraseñas de usuarios Autenticación de usuarios para conexiones externas, Aislamiento de sistemas sensibles.
- Adquisición, desarrollo y mantenimiento de SI, tiene 16 controles: Validación de datos de entrada, Control de acceso al código fuente de los programas, control de vulnerabilidades técnicas
- Gestión de incidentes de seguridad de la información, con sólo 5 controles: Informes de eventos de seguridad, Recogida de pruebas, es sin embargo uno de los aspectos claves en la gestión de la seguridad de la información.
- Gestión de la continuidad del negocio, también con 5 controles: Evaluación de riesgos y continuidad del negocio, prueba, Mantenimiento y re-evaluación de los planes de continuidad.
- Es uno de los requisitos fundamental para cualquier SGSI.
- Conformidad, tienen 10 controles: Identificación de la legislación aplicable, Controles de auditoría de los sistemas de información.



Además de la ISO 27000, se debe tomar una versión aplicable de una de las normas siguientes, que gozan de aceptación internacional:

- Organización Internacional de Normalización 17799/Norma británica 7799: *Code of practice for Information Security Management* (ISO/IEC 27002).
- *Bundesamt fuer Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch* (IT Protection Manual).
- *Information Systems Audit and Control Foundation*: objetivos de control en el ámbito de la información y las tecnologías afines (COBIT).

Las medidas de seguridad deberán estar adaptadas a la estructura administrativa, al personal y al entorno tecnológico de cada organismo pagador. El esfuerzo financiero y tecnológico deberá ser proporcional a los riesgos reales.

Proceso de Auditoría Informática.

El proceso de auditoría requiere de algunos aspectos básicos tales como:

1. Perfil del Auditor: Es un profesional dedicado al análisis de sistemas de información e informáticos que esta especializado en algunas de las múltiples ramas de la auditoria informática, que tiene conocimientos generales y que además posea las características necesarias para actuar como consultor con su auditado, dándole ideas de cómo enfocar la construcción de los elementos de control y de gestión.

   Las personas que integren la función de Auditoria Informática, deben contemplar en su formación básica una mezcla de conocimientos de auditoria financiera y de auditoría informática general.

2. Conocimientos básicos:
   - 2.1. Desarrollo informático; gestión de proyectos y del ciclo de vida de un proyecto de desarrollo.
   - 2.2. Gestión del Departamento de Sistemas.
   - 2.3. Análisis de riesgos en un entorno informático.
   - 2.4. Sistema operativo (este aspecto dependerá de varios factores, pero principalmente de si va a trabajar en un entorno único-auditor interno- o, por el contrario va a tener posibilidades de trabajar en varios entornos como auditor externo).
   - 2.5. Telecomunicaciones
   - 2.6. Gestión de bases de datos
   - 2.7. Redes locales
   - 2.8. Seguridad física
   - 2.9. Operación y planificación informática

2.10. Gestión de la seguridad de los sistemas y de la continuidad empresarial

2.11. Gestión de problemas y de cambios en entornos informáticos

2.12. Administración de datos

2.13. Ofimática

2.14. Comercio electrónico

2.15. Encriptación de datos.

Dependiendo del tipo de auditoria a realizar se deben analizar los perfiles profesionales que se requieren para el personal que desarrollará del trabajo de auditoria. A continuación se presenta un cuadro referencial con esto perfiles profesionales.

Perfiles Profesionales de los auditores informáticos

Profesión	Actividades y conocimientos deseables
Informático	Con experiencia amplia en distintas ramas. Que sus labores se hayan desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación

Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.

Fuente: Cavandes (2002). Argentina

3. Investigación Preliminar

Esta etapa es de suma importancia para el buen desarrollo de la auditoria puesto que es de desear que en esta investigación preliminar se obtengan aspectos previos que proporcionen datos necesarios para el conocimiento de la organización y de los sistemas de información que se van ha auditar. A continuación se especifican algunas estrategias a considerar en la investigación preliminar.

3.1. Objetivos:

3.1.1. Conocer los recursos informáticos de la empresa y la estructura organizacional de esta.

3.1.2. Evaluar la importancia del sistema de información para los procesos del negocio objeto de la auditoria y el soporte que los recursos de informática dan a estos.

3.1.3. Conocer de manera global el sistema informático sobre el cual se llevará a cabo la auditoria, identificando los elementos que apoyan la seguridad y administración.

3.2. Consideraciones:

3.2.1. Conocimiento global de la empresa en cuanto a:

3.2.1.1. Área de Tecnología de la Información (Área de sistemas)

Estructura organizacional y personal

Plataforma de hardware

Sistemas operativos

Sistemas de redes y comunicaciones

3.2.2. Conocimiento global del sistema informático, evaluando las herramientas que proporciona como apoyo a la seguridad y a la administración.

3.3. Técnicas y Herramientas que se utilizan para la realización de la Investigación Preliminar:

3.3.1. Entrevistas previas con el cliente (persona que solicita la realización de la auditoria).

3.3.2. Inspección de las instalaciones donde se llevará a cabo la auditoria y observación de operaciones.

3.3.3. Investigación e indagación con el personal involucrado en el proyecto de auditoria y los funcionarios que administran y operan los sistemas a evaluar.

3.3.4. Revisión de documentación proporcionada por la empresa.

3.3.5. Revisión de informes de auditorias anteriores, si se han realizado.

3.3.6. Estudio y evaluación del sistema de control interno.

3.4. Documentos a solicitar para la Investigación Preliminar

3.4.1. Listado de aplicaciones en producción y directorio de datos.

3.4.2. Documento de autorización a cada usuario del sistema y aprobación de derechos y privilegios.

3.4.3. Listados de monitoreo del sistema.

3.4.4. Listado de utilidades importantes, con los usuarios y grupos que las acceden.

3.4.5. Políticas, estándares, normas y procedimientos.

3.4.6. Manuales de sistemas

3.4.7. Documento de configuración inicial del sistema y las autorizaciones para su actualización o cambio.

3.4.8. Documento de definición de los roles en la administración del sistema y la seguridad.

3.4.9. Contratos, pólizas de seguros

3.4.10. Planes de capacitación y entrenamiento.

3.4.11. Contratos con entes externos relacionados con Tecnologías de la Información.

3.4.12 Informes de auditoría previos.

4. Personal Participante en el trabajo de Auditoria Informática.

La cantidad de recursos depende del volumen de la auditoria. Las características y perfiles del personal seleccionado dependen de la materia auditable. Es importante mencionar que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Aspectos Generales de la Auditoría.

Propuesta de Auditoría

1. Estimación de Honorarios.

En lo que respecta a la presentación de la propuesta se debe cumplir la investigación previa a los fines de determinar el alcance de la auditoría, tomado en cuenta esto la firma de auditoria procede a estimar en función del trabajo a realizar y del personal ejecutor de la auditoria, sus honorarios profesionales y de la auditoria, para lo cual se pueden utilizar los formatos que se incluyen como Anexo A.

1.1. Horas-Hombre para la realización de trabajo de Auditoría.

1.2. Distribución Porcentual del Tiempo.

1.3. Presupuesto: Está conformado por los Honorarios Profesionales, Honorarios por Servicio de Auditoría, otros gastos (viáticos, gastos de papelería, copias etc.)

2. El Contrato

El Auditor deberá acordar por escrito con su cliente el objetivo y alcance del trabajo, así como sus honorarios o los criterios para su cálculo para todo el período de nombramiento.

El Contrato se materializa mediante:

- La Firma de un documento o contrato.
- Carta de Aceptación.

El contrato no tiene una estructura fija definida, sin embargo puede decirse en líneas generales que el mismo debe incluir al menos los siguientes aspectos:

2.1. Entidad auditada

Entidad que solicita la auditoría informática.

2.2. Debe quedar por escrito el compromiso que tienen las empresas o entidades auditadas las cuales estarán obligadas a facilitar cuanta información fuera necesaria para realizar los trabajos de auditoría; asimismo, quien o quienes realicen dichos trabajos estarán obligados a requerir cuanta información precisen para la emisión del informe de auditoría.

2.3. También de especificarse la responsabilidad que tiene el auditor

Auditor informático:

- Sujetos a normas que tipifican su capacidad profesional.
- Obtener evidencias suficientes y adecuadas.
- Evaluar controles, riesgos.

2.4. Se deben identificar las Terceras partes, es decir Terceros que mantienen relación con la entidad auditada, en materia de informática de ser el caso.

2.5. Objeto del Contrato

En el objeto del contrato de auditoría o carta de aceptación se establece las condiciones bajo las cuales se llevará a cabo la auditoría.

2.6. Alcance

Motivo que justifica la auditoria y hasta donde se va abarcar en el trabajo de auditoria.

2.7. Información Y Responsabilidad

El auditor tiene la obligación de comunicar por escrito a la Dirección de la entidad auditada, las debilidades significativas de control interno identificadas en la ejecución de su trabajo.

2.8. Plazos y Planificación:

2.8.1. Planes de trabajo y fecha de entrega de documentos.

2.8.2. Identificación de los destinatarios del informe.

2.8.3. Acuerdos de grado de colaboración de los auditores internos y personal interno

2.9. Horas y Periodo de Contratación:

2.9.1. Horas estimadas para la realización del trabajo.

2.9.2. Honorarios.

2.9.3. Condiciones de pago.

2.9.4. Periodo de contratación.

ASPECTOS LEGALES.

EL DERECHO INFORMÁTICO.

De acuerdo a Peñaranda (2001). “Es el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en dos aspectos: a) Regulación del medio informático en su expansión y desarrollo y b) Aplicación idónea de los instrumentos informáticos”; es decir involucra hechos y actos producido por el hombre

en el área de informática y que deben ser regulados y controlados, a través de leyes y principios.

Carácter del Derecho Informático:

El derecho informático, tiene carácter público por su relación directa con el Estado, pero también posee carácter privado puesto que por tratarse entre particulares con la libertad de hacerlo, el acuerdo de voluntades se materializa mediante un contrato, que por su naturaleza y pautas se acoge a la tutela del Derecho Público.

Ramas del derecho con que se relaciona:

El Derecho Informático se relaciona con el Derecho Constitucional, el Derecho Penal, con los Derechos Humanos y con la Propiedad Intelectual.

Es de importancia realizar un breve comentario sobre la Propiedad Intelectual, especialmente en relación a Venezuela, que necesita mejorar el control en ésta materia, para penalizar de acuerdo a lo que establece Peñaranda (2001) "…. plagios, la piratería y en si cualquier ilícito en contra de los derechos de autor o industriales, debido a que se están produciendo éstos en contra y por medio de los instrumentos informáticos."

A continuación se presenta un pequeño análisis sobre las leyes venezolanas que regulan el área informática en Venezuela, mencionado aspectos de interés para la Auditoria Informática.

LEYES VENEZOLANAS.

Ley Orgánica de Ciencia, Tecnología e Innovación.

Ley sobre Mensajes de Datos y Firmas Electrónicas.

Ley Especial Contra Delitos Informáticos.

Ley de Tecnologías de Información.

Ley Orgánica de Telecomunicaciones

Ley del Derecho del Autor y La Autora y Derechos Conexos.

LEY	Aspectos a considerar en una auditoría
Ley sobre mensajes de datos y firmas electrónicas.	Contempla en sus artículos 16, 17 y 18, aspectos sobre las firmas electrónicas tales como: Validez y eficacia de la Firma Electrónica. Requisitos, Efectos jurídicos. Sana critica, La certificación**.** Obligaciones del signatario. Capitulo VII. Artículos del 38 al 34. Certificados Electrónicos.
Ley especial contra delitos informáticos.	Permite conocer los delitos tipificados en la Ley tales como: • Delitos Contra los Sistemas que Utilizan Tecnologías de Información (artículos 6 al 12) • Delitos Contra la Propiedad (artículos 13 al 19) • Delitos contra la privacidad de las personas y de las comunicaciones (artículos 20 al 22). • De los delitos contra niños, niñas o adolescentes (Artículos 23 y 24) • Delitos contra el orden económico (artículos 25 y 26)
Ley Orgánica de Telecomunicaciones	Constituye una guía para verificar entre otras cosas lo siguiente: • De los derechos y deberes de los usuarios (Artículos 12 y 13). • De los derechos y deberes de los operadores. (Artículos 14 y 15). • De la prestación de servicios y del establecimiento y explotación de redes de telecomunicaciones (Artículos 16 al 24) • Del procedimiento para la obtención de habilitaciones administrativas o la

	incorporación de atributos a las mismas (Artículos del 25 al 33). • Del procedimiento para la concesión de uso y explotación del espectro radioeléctrico. (Artículos 76 y 77).
Ley de Tecnologías de Información	Aspectos a considerar: • Del uso de las tecnologías de información en el poder público (artículos 17 al 34) • De la seguridad de los sistemas y las redes, y del riesgo tecnológico (artículos 37 y 38) • Derechos y garantías de los ciudadanos (Artículos 66 al 74) • De los sistemas, programas y aplicaciones informáticos del poder público (Artículos 75 al 80) • De las sanciones. (Artículos 83 al 89)
Ley de derecho de autor y la autora y derechos conexos.	Interesa al trabajo de Auditoria: • Los límites de los derechos de comercialización (Artículos 44 al 49). • Los documentos que deben registrarse. (Artículos 100 al 104).

Para Ramos González, citado por Peñaranda (2001), en su libro Iuscibernética: Interrelación entre el Derecho y la Informática, define a la auditoria informática como:

> La Auditoria Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes del entorno informático de una entidad, abarcando todas o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables; el grado se satisfacción de usuarios y directivos; los controles existentes y una análisis de riesgos. (p.40)

En consecuencia la Auditoria Informática es la revisión y la evaluación de los controles, sistemas, procedimientos del área de informática; además incluye la evaluación de los equipos de computación, su utilización, eficiencia y seguridad, de la organización y del personal que participa en el procesamiento de la información, a fin de que por medio de estrategias y de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Por otra parte, la auditoria informática sustenta y confirma la obtención de los objetivos tradicionales de la auditoria como son: Objetivos de protección de activos e integridad de datos y Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficiencia y eficacia.

En los términos antes planteados el auditor informático debe planear para el logro de los objetivos de auditoria, la revisión y evaluación del Control Interno Informático, que según Piattini y Del Peso (2001), se puede definir 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 conseguir sus objetivos” (p.30), toda vez que cuando se diseñan, se desarrollan e implantan los controles, han de ser completos, fiables, adecuados etc.

Ante la diversidad en el alcance de la auditoria informática, como lo es la seguridad, control interno informático, eficiencia y eficacia, tecnología informática, continuidad de operaciones y gestión de riesgos, tomando en cuenta sus relaciones e implicaciones operativas que tienen los sistemas en el contexto empresarial, conviene mencionar algunos tipos de Auditoria Informática, donde se muestra las áreas auditables en esta materia, los cuales puede ser: Auditoria de Dirección, Auditoria de Seguridad, Auditoria de Base de Datos, Auditoria de Explotación, Auditoria de Calidad, Auditoria del Desarrollo, Auditoria de Mantenimiento, Auditoria de Redes, entre otras.

Auditoría de Dirección

Este tipo de auditoria evalúa la Organización y valoración de la dirección de Informática, el Plan Estratégico de los Sistemas de Información, el Análisis de cargos, Planes y Procedimientos, Normativa y Gestión Económica.

Auditoría de Seguridad

Comprende la evaluación de la seguridad física, lógica, organizativo-administrativa y jurídica. En cuanto a la Auditoria de Seguridad Física le interesa la revisión de las políticas y Normas sobre seguridad Física, verificación de la seguridad del personal, datos, hardware, software e instalaciones, seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente Informático. En la Lógica: evalúa la protección que debe tener el patrimonio informático (aplicaciones, bases de datos y ficheros). En la Organizativo-administrativa se evalúa la existencia de políticas de seguridad informática, políticas de personal, los análisis de riesgos y planes de contingencia y en la Jurídica, la revisión del marco jurídico que regula el área de Informática.

Auditoría de Base de Datos

Revisa la confiabilidad, el acceso, la seguridad, las restricciones en materia de base de datos del sistema informático auditado.

Auditoría de Explotación

Auditar Explotación consiste en auditar las secciones que la componen y sus interrelaciones. La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico.

Auditoría de Calidad

Revisión del Sistema de Calidad del área de informática, que comprende la observación de los controles que han sido aplicados, Evaluación de la calidad de los datos obtenidos, Verificación de

Normativas o Estándares de Calidad Fondonorma, Normas ISO 12207: Calidad en los procesos del ciclo de vida del software 9126: característica de calidad de un producto de software.

Auditoría del Desarrollo

Comprende la evaluación de los proyectos en desarrollo, 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.

Auditoría de Mantenimiento

Comprende la revisión de la evaluación y control del mantenimiento del software.

Auditoría de Redes

Auditoría de Red indicará, con toda precisión, asuntos clave relacionados con la red, mostrando dónde las nuevas aplicaciones empresariales van a generar nuevas demandas de red, no se limita a un análisis de la infraestructura física de la red y a los sistemas operativos de la misma. Su diseño es específico para cada empresa y tiene en cuenta aspectos que incluyen técnicas de control de funcionamiento, suministro de información, medidas de seguridad y análisis de coste y de riesgo.

Toda auditoría para poder llevarse a cabo debe seguir un proceso de organización y planeación.

PLANEACIÓN DE LA AUDITORÍA INFORMÁTICA.

Para realizar una planeación de la Auditoria Informática, deben cumplirse una serie de pasos previos, a los fines de dimensionar y caracterizar el área objeto de auditoria, incluyendo sus sistemas, organización y equipos de computación.

La planeación de una auditoria informática debe hacerse desde las perspectivas de los objetivos de auditoria planteados, es decir tomado en cuenta por ejemplo la evaluación de los sistemas y sus procedimientos, además de los equipos con que se cuenta.

Es este sentido para realizar una buena planeación de la auditoria informática, debe obtenerse información general de la organización y de la función informática a evaluar.

Por lo anterior podría decirse entonces que se pueden cumplir las siguientes etapas:

Etapa 1. Definición de Alcance y Objetivos:

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

Etapa 2. Preliminar o Diagnóstico:

Esta etapa comprende el proceso de Investigación Preliminar que fue detallado anteriormente. Sin embargo es importante señalar que ésta investigación preliminar comprende: El conocimiento del negocio, conocer el nivel de apoyo de la función informática al negocio, áreas de oportunidad y el diagnóstico del área de informática. Para llevar a cabo esta etapa el auditor debe

utilizar herramientas tales como la observación, utilización de cuestionarios, entrevistas, Checklist entre otras.

Etapa 3. Evaluación del Control Interno:

De acuerdo a lo planteado en el Control Interno Informático se detalla los procesos y métodos a seguir en ésta evaluación.

Etapa 4. Evaluación de Riesgos:

Una vez finalizada la investigación preliminar y la evaluación del control interno, se debe obtener documentos fundamentales que justifican la realización de la Auditoria Informática, tales como: Matriz de Riegos, plan de la auditoria y la carta de aceptación o de contrato.

Matriz de Riesgos: Tiene como objetivo principal detectar las áreas de mayor peligro en relación con informática y que requieren una revisión formal y oportuna. Ejemplos de las áreas susceptibles de auditoría:

Administración de informática (misión, organización, servicios, etc.)

Usuarios de informática (comunicación e integración, proyectos conjuntos)

Sistemas de información (planeación, desarrollo, operación)

Mantenimiento (hardware, software, telecomunicaciones)

Redes locales (administración, instalación, operación/seguridad)

Software (administración y legalización de lenguajes de programación, sistemas operativos)

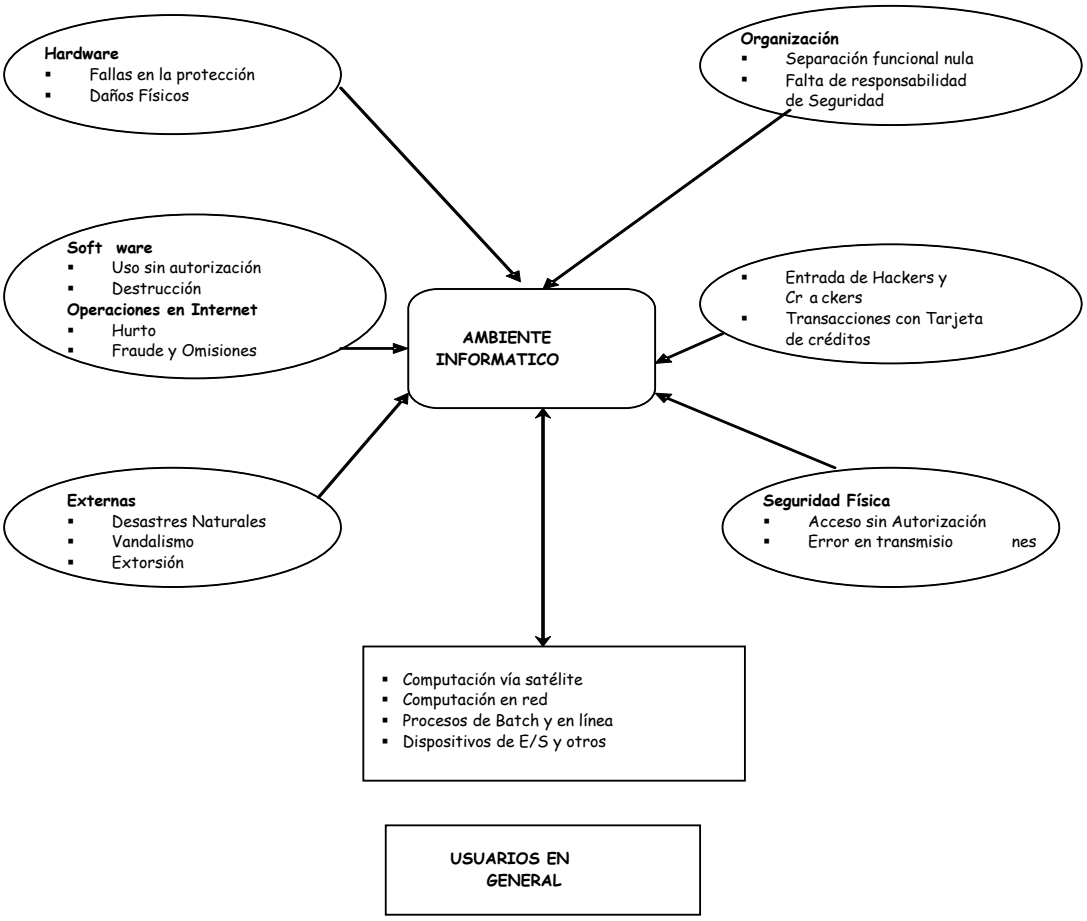
Seguridad (hardware, software/aplicaciones)

Investigación tecnológica (metodologías, técnicas, herramientas, capacitación)

Procedimiento de análisis y elaboración de la matriz: Es importante identificar el nivel de riesgo de cada uno de los elementos en el

negocio a través del diagnóstico de la situación actual del área de informática. Las áreas a diagnosticar pueden variar según el tamaño y estructura del negocio.

El auditor debe utilizar los elementos de medición y evaluación posibles sin caer en un análisis detallado, ya que solo se trata de detectar la problemática principal de cada área. Para lo cual se hace necesario definir el ambiente informático (Ver fig. No.1), a los fines de definir las principales amenazas que lo afectan, lógicamente esta definición irá en función área que se audita. Posterior a la definición del ambiente informático y sus principales amenazas se puede establecer la ponderación del riesgo y la matriz de riesgo.



FUENTE. Figura 1. Principales amenazas que afectan el ambiente informático.

Etapa 5. Ejecución de la Auditoría.

La etapa de ejecución debe cumplirse tomando en cuenta lo planificado, dicha ejecución se hará de acuerdo al tipo de auditoria y puede cumplir los siguientes pasos, los cuales deben quedar especificados en el Programa de Auditoría Informática (Plan de Trabajo) respectivo.

Proceso de Elaboración del sistema (s) a auditar.

Se debe evaluar en forma detallada el proceso de elaboración del sistema a auditar, tomando en cuenta los siguientes aspectos:

Verificar la existencia de sistemas interconectados como un todo o si por el contrario existen programas independientes.

Determinar si la elaboración del sistema auditado se hizo obedeciendo a un plan estratégico (servicios, disposición de uso, características, recursos), o no se tomó en cuenta prioridades y objetivos.

Revisión del 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 (costo-beneficio)

Evaluación de Análisis.

Evaluar 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: Planeación estratégica, requerimientos de usuarios e inventario de sistemas.

Evaluación del diseño lógico del sistema

En ésta etapa se debe evaluar las especificaciones del sistema, al tener el análisis del diseño lógico del sistema se compara con lo que realmente se está obteniendo por lo que también se debe evaluar lo planeado. 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:

1. Manual del usuario.
   1.1. Descripción de flujo de información y/o procesos.
   1.2. Descripción y distribución de información.
   1.3. Manual de formas.
   1.4. Manual de reportes.
   1.5. Lista de archivos y especificaciones.
   1.6. Lo que se debe determinar en el sistema:
2. En el Procedimiento.
   2.1. ¿Quién hace, cuando y como?
   2.2. ¿Qué formas se utilizan en el sistema?
   2.3. ¿Son necesarias, se usan, están duplicadas?
   2.4. ¿El número de copias es el adecuado?
   2.5. ¿Existen puntos de control o faltan?
3. En la gráfica de flujo de información
   3.1. ¿Es fácil de usar?
   3.2. ¿Es lógica?

3.3. ¿Se encontraron lagunas?

3.4. ¿Hay faltas de control?

4. En el diseño.

4.1. ¿Cómo se usará la herramienta de diseño si existe?

4.2. ¿Qué tan bien se ajusta la herramienta al procedimiento?

Todo lo anterior se hace necesario para verificar entre otras cosas el adecuado funcionamiento de los sistemas. Tal y como se plantea en la siguiente tabla, tomada del libro Sistemas de Información Gerencial de Laudon y Laudon.

ESPECIFICACIONES DE DISEÑO	
SALIDA – Medio – Contenido – Oportunidad	**CONTROLES** – Controles de entrada (caracteres, límite, moderación). – Controles de procedimiento (consistencia, conteos de registro). – Controles de salida (totales, muestras de salida). – Controles de procedimientos (contraseñas, formularios especiales).
ENTRADA – Orígenes – Flujo – Introducción de datos	**SEGURIDAD** – Controles de acceso – Planes de catástrofe – Referencias de Auditoría

ESPECIFICACIONES DE DISEÑO	
INTERFAZ DEL USUARIO – Sencillez – Eficiencia – Lógica – Retroalimentación – Errores	**DOCUMENTACIÓN** – Documentación de Operaciones – Documentación de Sistemas – Documentación del Usuario
DISEÑO DE LA BASE DE DATOS – Modelos de datos lógicos – Requerimientos de volumen	**CONVERSIÓN** – Transferir archivos – Iniciar nuevos procedimientos

y velocidad – Organización y diseño de archivos – Especificaciones de registro	– Seleccionar método de prueba – Reducir al nuevo sistema
PROCESAMIENTO – Cálculos – Módulos de programas – Informes requeridos – Oportunidad de las salidas	**CAPACITACIÓN** – Seleccionar las técnicas de capacitación – Desarrollar los módulos de capacitación – Identificar las instalaciones de capacitación
PROCESAMIENTOS MANUALES – Qué actividades – Quién las realiza – Cuándo – Cómo – Dónde	**CAMBIOS ORGANIZACIONALES** – Rediseño de tarea – Diseño de puesto de trabajo – Diseño de proceso – Diseño de estructura de la organización – Relaciones de Informes

Fuente: Laudon y Laudon (2004). Pág 391.

En esta etapa se realizan en general las siguientes actividades:

- Aplicación del cuestionario al personal.
- Entrevistas a líderes y usuarios mas relevantes de la dirección.
- Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos.
- Evaluación de la estructura orgánica: departamentos, puestos, funciones, autoridad y responsabilidades.
- Evaluación de los Recursos Humanos y de la situación Presupuestal y Financiera: desempeño, capacitación, condiciones de trabajo, recursos en materiales y financieros mobiliario y equipos.
- Evaluación de los sistemas: relevamiento de Hardware y Software, evaluación del diseño lógico y del desarrollo del sistema.
- Evaluación del Proceso de Datos y de los Equipos de Cómputos: seguridad de los datos, control de operación, seguridad física y procedimientos de respaldo.

Basado en lo planteado, se deben aplicar pruebas sustantivas y de cumplimiento, las cuales consisten en lo siguiente:

El objetivo de las pruebas sustantivas es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir pérdidas materiales durante el proceso de la información.

Se pueden identificar 8 diferentes pruebas sustantivas:

- Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.
- Prueba para asegurar la calidad de los datos.
- Pruebas para identificar la inconsistencia de datos.
- Prueba para comparar con los datos o contadores físicos.
- Confirmación de datos con fuentes externas
- Pruebas para confirmar la adecuada comunicación.
- Prueba para determinar falta de seguridad.
- Pruebas para determinar problemas de legalidad.

El objetivo de las pruebas de cumplimiento, es determinar si el control interno es adecuado y si está en funcionamiento en la forma que se planteó en el área de informática.

Las pruebas de cumplimiento deben apoyarse en el alcance que se determinó quedando soportado en:

- La documentación.
- Manuales de usuarios, técnicos y procedimientos
- Cambios en los programas
- Solicitudes por escrito
- En pruebas por parte de los usuarios.
- Actualización de los manuales técnicos y de usuarios
- Verificar que los cambios en los programas sean realizados por el personal de informática o por el proveedor de la aplicación.
- Copias de respaldo y recuperaciones.

- Contenidos de las copias.
- Periodicidad de las copias.
- Persona responsable.
- Custodia, almacenamiento, inventario, rotación de la cinta.
- Acceso a datos y programas.
- Verificar la lista de usuarios que tiene acceso.
- Revisar el procedimiento para otorgar y eliminar los accesos.
- Analizar la periodicidad de los cambios de los passwords (clave).
- Capacitación de los usuarios
- Controles en la entrada, proceso y salida

Etapa 6. Revisión y pre-informe.

- Revisión de los papeles de trabajo.
- Determinación del Diagnóstico e Implicancias.
- Elaboración de la Carta de Gerencia.
- Elaboración del Borrador.

Etapa 7. Informe

Elaboración y presentación del Informe.

CAPITULO III

MARCO METODOLÓGICO

El presente capítulo incluye, la naturaleza de estudio que detalla el tipo y modalidad de investigación y los procedimientos seguidos para el logro de los objetivos de investigación

Tipo y Diseño de la Investigación

El estudio se basa en una investigación de campo tipo descriptivo ya que los datos fueron recogidos en forma directa de la realidad, con el fin de describirlos e interpretarlos y se ubica dentro del tipo de investigación de carácter analítico, descriptivo y explicativo. A tal efecto de acuerdo con Hernández S. y otros (2000). Los estudios descriptivos "buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis" (p. 60), los estudios explicativos van mas allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; están dirigidos a responder a las causas de los elementos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en que condiciones se da éste.

La investigación es de carácter descriptivo porque se presenta la situación o se describen los procedimientos utilizados por los ingenieros, auditores para realizar las investigaciones en el área de auditoria informática.

De la misma forma, es un estudio explicativo, por cuanto se detectaron o se determinaron los diferentes escenarios de sistemas de información susceptibles de una Auditoria Informática, mediante los cuales se pudo formular un Modelo de Auditoria Informática para la evaluación de los Sistemas de Información.

Población

La investigación trata dos universos objetos de estudio, un primer universo está conformado por los profesionales del área de la Informática, ubicados en ramo de las empresas de servicios que comercializan con sistemas de información y con experiencia en auditoria informática.

Un segundo universo lo constituyen los usuarios de estos sistemas en los diferentes ramos empresariales, clasificados de acuerdo a sus características en jurisdicción del Municipio Iribarren, Barquisimeto Estado Lara.

Muestra

Se tomó para el I estrato un total de 10 profesionales en el área de la Informática, ubicados en ramo de las empresas de servicios que comercializan con sistemas de información y con experiencia en auditoria informática. En el segundo caso se analizaron 9 casos de empresas a las que se les aplico la metodología de auditoría.

Técnicas e Instrumentos de Recolección de Datos

La información recolectada tanto del cuestionario como de la guía de observación se ordenó y tabuló aplicando el programa estadístico SPSS bajo ambiente Windows versión 11.0. La información se presentó en tablas estadísticas y gráficas para describir la situación plateada. Por otra parte, las variables cuantitativas fueron analizadas mediante la Media Aritmética y la Desviación Estándar, las variables cualitativas se analizaron a través de las proporciones (frecuencias relativas). Además se utilizó la herramienta que facilitó la toma de decisiones como lo es el análisis de sensibilidad, el cual permitió diseñar escenarios en los cuales se pudo analizar los resultados del proyecto, cambiando los valores de sus variables y restricciones financieras y determinando cómo estas afectaron el resultado final.

Naturaleza del Estudio

El presente trabajo, se enmarca dentro del tipo descriptivo, que según Hurtado (1998) “tiene como objetivo central lograr la descripción o caracterización del evento de estudio dentro de un contexto particular”. (p. 213). Como variante, se orienta según los diseños “transeccionales”, definidos como “aquellos en los cuales el interés del investigador se centra en describir el evento en un momento único en el tiempo presente”. (ob. cit., p. 219). Es decir, los diseños de investigación “transeccionales” descriptivos, también denominados transversales, “recolectan datos en un sólo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado”. (Hernández et. al., 1991). Por otra parte el trabajo se desarrolló a través de dos modalidades de Investigación la de Campo, que según Barrios y otros (1998) se entiende como:

> El análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo... (p. 5).

Tomando en cuenta que se evaluaron estrategias de enseñanza-aprendizaje ya practicadas en las clases de Auditoria Informática, y por la otra también se enmarca dentro de la modalidad de Proyecto Factible el cual es una “propuesta sustentada en un modelo viable, para resolver problemas prácticos planteados, tendientes a satisfacer necesidades institucionales o sociales y pueden referirse a la formulación de políticas (p.16), (Barrios 1998), dado que se presenta propuesta sobre de estrategias de enseñanza-aprendizaje que se adapten a las particularidades del proceso enseñanza-aprendizaje de la auditoria informática.

Procedimientos

Para el logro del Objetivo Especifico No. 1, Conocer los aspectos legales que regulan la Auditoría Informática, se revisó toda la bibliografía nacional e internacional, en esta materia.

En cuanto al Objetivo Especifico No. 2, Diagnosticar los escenarios posibles, analizar posibles resultados y revisar los Sistemas de Información susceptibles para la realización de Auditorías Informáticas, se realizó lo siguiente:

- Fueron seleccionado 9 casos empresariales.
- Se les aplico la metodología de auditoria informática.
- Los resultados fueron tabulados y analizados, presentando los hallazgos de auditoría.
- Se presentaron las conclusiones y recomendaciones.

Para el logro del Objetivo Específico No.3, Identificar los riesgos potenciales y la seguridad física de los sistemas de información, fue revisada la bibliografía correspondiente, planteando la metodología para identificar los mismos.

En cuanto al Objetivo Específico No.4 Describir los procedimientos sustantivos y de control a seguir para la evaluación de los sistemas de información, queda demostrado en los casos de las empresas auditadas.

Finalmente para el Objetivo Específico No. 5 Proponer una Metodología de Auditoría para la revisión de los Sistemas de Información, fue revisada bibliografía al respecto, se utilizó los resultados del cuestionario aplicado a Profesionales en el área de Informática y se analizó experiencias de auditoría informática. Quedando dicha propuesta estructurada de la siguiente manera:

- Presentación de la Propuesta.
- Fundamentación.
- Definición de la metodología
- Misión y Visión
- Filosofía de Gestión de la Metodología.

- Objetivos Específicos
- Objetivos Estratégicos
- Justificación
- Componentes
- Operatividad.
- Simulación
- Estructura de la Metodología.

Sistema de Variables

Definición Conceptual

OBJETIVOS ESPECIFICOS	VARIABLE	DEFINICIÓN CONCEPTUAL
(1) Conocer los aspectos legales que regulan la Auditoría Informática.	Aspectos Legales	Leyes y Normas que regulan los procesos de Auditoria Informática.
(2) Diagnosticar los escenarios posibles, analizar resultados y revisar los Sistemas de Información susceptibles para la realización de Auditorías Informáticas.	Sistemas de Información	Un sistema de información es un conjunto organizado de elementos, que pueden ser personas, datos, actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.
	Auditoría Informática	Según la enciclopedia Wikipedia. La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en 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, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

OBJETIVOS ESPECIFICOS	VARIABLE	DEFINICIÓN CONCEPTUAL
(3) Identificar los riesgos potenciales y la seguridad de información.	Riesgos	Riesgo es una eventualidad que imposibilita el cumplimiento de un objetivo.
	Seguridad de la Información	La seguridad de la información, se puede definir como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.
(4) Describir los procedimientos sustantivos y de control a seguir para la evaluación de los sistemas de información.	Procedimientos Sustantivos	Procedimientos Sustantivos, son los pasos a seguir para realizar las "Pruebas sustantivas" que verifican la exactitud, integridad y validez de la información.
	Procedimientos de Control	Procedimientos de Control son los pasos a seguir para realizar las "Pruebas de cumplimiento" las cuales determinan si un sistema de control interno funciona adecuadamente (según la documentación, según declaran los auditados, según las políticas y procedimientos de la organización (normativa interna, códigos tipo, etc.), según los estándares externos o incluso según las certificaciones obtenidas en el pasado), es decir, lo que se quiera contratar para comprobar si se cumple.
(5) Proponer una Metodología de Auditoria para la revisión de los sistemas de información.	Metodología	Según el diccionario de la Real Academia Española (RAE), una metodología es un conjunto de acciones o pasos debidamente sistematizados.

Definición Operacional

OBJETIVOS ESPECÍFICOS	DIMENSIÓN	INDICADOR	INSTRUMENTO
(1) Conocer los aspectos legales que regulan la Auditoria Informática.	Aspectos Legales	Normas y leyes	Revisión Bibliográfica acerca del Marco Legal
(2) Diagnosticar los escenarios posibles, analizar resultados y revisar los Sistemas de Información susceptibles para la realización de Auditorías Informáticas.	Sistemas de Información Auditoria Informática	Escenarios Empresariales Informes de Auditoria	Realización de auditorías en nueve (09) organizaciones, aplicación de procedimientos de auditoría y emisión de informes de auditoria
(3) Identificar los riesgos potenciales y la seguridad de información.	Riesgos Seguridad de la Información	-Amenazas -Vulnerabilidad -Impacto -Vulnerabilidad -Confidencialidad -Integridad -Disponibilidad	Revisión Bibliográfica sobre Riesgos y Seguridad de la información
(4) Describir los procedimientos sustantivos y de control a seguir para la revisión de los sistemas de información.	Procedimientos Sustantivos Pruebas de Cumplimiento	-Diseño de Pruebas Sustantivas -Diseño de Pruebas de Cumplimiento	Formatos Cuestionarios Programas específicos
(5) Proponer una Metodología de Auditoria para la revisión de los sistemas de información.	Metodología	Propuesta	Cuestionario aplicado a Profesionales en el área de Informática. Revisiones Bibliográficas, experiencias de auditoria informática

CAPITULO IV

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS

A continuación se presenta la descripción del análisis e interpretación de los resultados obtenidos y la demostración del cumplimiento de los objetivos propuestos en el presente trabajo de investigación.

Objetivo No. 1: Conocer los aspectos legales que regulan la Auditoria Informática.

En el Capítulo II. Marco Teórico queda explícitamente analizado y revisado todo el marco legal que regula en materia de Sistemas de Información y Auditoria Informática.

Objetivo No. 2: Diagnosticar los escenarios posibles, analizar resultados y revisar los Sistemas de Información susceptibles para la realización de Auditorías Informáticas.

De seguidas se describen los resultados de las auditorías realizadas, detallando por tipo de auditoría informática, los escenarios auditados.

4.1. Escenario No. 1:

Tipo de Auditoría Informática: Dirección

Empresa: Dirección de Informática de la UCLA.

Programa de Auditoria Informática de Dirección aplicado.

- Visita Preliminar
  - Solicitud de Manuales y Reglamentos.
  - Entrevista a líderes y usuarios más relevante de la dirección.
  - Elaboración de los cuestionarios de control interno.

- Recopilación de la información organizacional: organigrama y manuales de funciones, recursos humanos, políticas.

– Desarrollo de la Auditoría
  - Aplicación del cuestionario.
  - Evaluación de la estructura orgánica: departamentos, puesto, funciones, autoridad y responsabilidad.
  - Evaluación de los recursos humanos: desempeño, capacitación, condiciones de trabajo, recursos en materiales mobiliario y equipos.
  - Análisis de la información.
  - Debilidades y fortalezas
– Revisión y Elaboración del Informe
  - Revisión de los papeles de trabajo.
  - Determinación del diagnostico e implicancias
  - Elaboración del informe
– Evaluación del Control Interno

Resultados de la aplicación del cuestionario de control interno al personal de la Dirección de Informática de la UCLA. (Anexo A)

ÍTEM	SI	NO	N/A
1	89%	11%	
2	90%	10%	
3	70%	20%	10%
4	89%	11%	
5	20%	80%	
6	90%	10%	
7	10%	90%	

Ítem 1

Al consultar si la Dirección de Informática, desarrolla planes a corto, mediano y largo plazo que apoyen el logro de los objetivos, el 89% respondió afirmativamente y el 11% negativamente, por lo que se infiere que posee un Plan Estratégico a seguir.

Ítem 2

Se consultó al personal de la Dirección de Informática, si dispone de un Plan Estratégico de Tecnología de la Información, el 90% responde que si y el 10% que no, lo que indica que con este instrumento puede guiar sus acciones en un corto, mediano y largo plazo.

Ítem 3

Al consultar si en el proceso de planificación se presta atención a los establecido en el Plan Estratégico, el 70% dijo que si, el 20% no y 10% no aplica, puede decirse entonces que dicho plan guía el proceso de planificación de la Dirección de Informática.

Ítem 4

De la consulta sobre si los recursos asignados son suficientes para llevar a cabo las tareas y actividades de la planificación, el 89% responde afirmativamente y el 11% negativamente, lo que indica que la Universidad, si presta un buen apoyo presupuestario para el desarrollo de las actividades de ésta Dirección de Informática.

Ítem 5

En lo que respecta a la consulta si el espacio físico en el lugar de trabajo es adecuado, el 20 % dijo que si y el 80% que no, por lo que se observa que el espacio físico no es adecuado, en virtud de la cantidad de personal adscrito a la Dirección.

Ítem 6

En cuanto a si los equipos existen están acordes con la tecnología actual, los encuestados respondieron en un 90% que si y en un 10% que no, lo que indica que a pesar los constantes avances tecnológicos, la Dirección de Informática mantiene adecuadamente actualizados sus equipos de trabajo.

Ítem 7

En lo relacionado a que si se cuenta con el personal suficiente para la realización de todas actividades de la Dirección de Informática, el 10% piensa que si y un 90% que no, estos resultados permiten inferir que el actual personal que existe en esta Dirección, no es suficiente para cubrir la diversidad de actividades que ejecutan, puesto que tiene que además de desarrollar nuevos sistemas, deben brindar soporte técnico a todas las Unidades Académicos Administrativas de la Universidad Centroccidental “Lisandro Alvarado”.

Identificación de Riesgos

Para la identificación de los riesgos se siguió lo establecido en la siguiente matriz:

Matriz de Riesgo

Riesgo Inherente	Riesgo de Control			
	Bajo	Medio	Alto
Alto	Medio	Bajo	Bajo
Medio	Alto	Medio	Bajo
Bajo	Alto	Alto	Medio
	Riesgo de Detección		

De la cual se obtuvieron los siguientes resultados:

Riesgo de Control

- Cumplimiento de las normativas internas sobre el uso y optimización de las tecnologías y sistemas de información en la UCLA, este riesgo se considera bajo, toda vez que la Dirección de Informática de la UCLA, procura trabajar con apego total a las normativas existentes.

Riesgo de Detección

- Analizar las solicitudes referidas a la automatización de procesos operativos.
- Asesoría en cuanto a los sistemas factibles de ser desarrollados.
- Establecimiento de acuerdos de servicios.

- Es considerado alto, ya que no se cuenta con el personal suficiente para que realice las evaluaciones constantemente.

Riesgo Inherente

- Evaluación de los proyectos y establecimiento de prioridades.
- Incremento sostenido del nivel de satisfacción del usuario.
- Evaluación de las demandas de servicio.

También este riesgo es alto pues apunta a la necesidad de lograr que los proyectos que se realizan, cumplan a cabalidad con las demandas y necesidades de los clientes.

Conclusiones

En la Dirección de Informática de la UCLA no se evidencian grandes deficiencias, puesto que se ha observado que tiene buen manejo del personal, conocen claramente las normas y las funciones de cada uno de los que allí laboran. Se puede decir que con respecto a la Dirección de esta área no hay ninguna irregularidad o mal manejo que pueda requerir alguna corrección.

La sugerencia es con respecto al espacio físico de dicha área, ya que se considera pequeño para la cantidad de personas que laboran en el mismo. Por otra parte en algunos momentos el personal se hace insuficiente para cumplir con los diferentes requerimientos solicitados a esta área, puesto que atienden a todas las unidades de la UCLA y sería importante contar con más personal; con el fin de mejorar el desarrollo y el funcionamiento de la dirección.

Además se recomienda realizar evaluaciones constantes en el desarrollo de sistemas y al soporte técnico, a fin de minimizar los posibles riesgos existentes.

4.2. Escenario No. 2:

Tipo de Auditoría Informática: Seguridad Física

Empresa: UCLA. Dirección de Informática

Programa de Auditoria Informática de Seguridad Física aplicado.

- Visita Preliminar
  - Solicitud de Manuales y Reglamentos.
  - Elaboración de los cuestionarios.
  - Recopilación de la información organizacional: estructura orgánica, recursos humanos, presupuestos.
- Desarrollo de la Auditoría
  - Aplicación del cuestionario al personal.
  - Entrevistas a encargados del departamento, vigilantes y usuarios más relevantes del departamento.
  - Análisis del acceso al área, control, seguridad, confiabilidad y respaldos.
  - Evaluación de la estructura orgánica: departamentos, puestos, funciones, autoridad y responsabilidades.
  - Evaluación de los Recursos Humanos y de la situación Presupuestaria y Financiera: desempeño, capacitación, condiciones de trabajo, recursos en materiales y financieros, mobiliario y equipos.
  - Evaluación de los sistemas: relevamiento de Hardware
  - Evaluación de los Equipos de Cómputos: seguridad física y procedimientos de respaldo.
  - Visita técnica de comprobación de seguridad física de la instalación del Departamento de Informática.
  - Evaluación técnica del sistema eléctrico y ambiental de los equipos y del local utilizado.

- Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación.

- Revisión y Elaboración del Informe
  - Revisión de los papeles de trabajo.
  - Determinación del diagnostico e implicancias
  - Elaboración de la Carta de Gerencia.
  - Elaboración del Informe.

Esta auditoría comprendió el área de la Dirección de Informática del Ubicada en el Rectorado de la Universidad Centroccidental "Lisandro Alvarado", abarcando aspectos tales como:

- Política de Seguridad.
- Aspectos organizativos para la seguridad.
- Seguridad ligada al personal.
- Seguridad física y del entorno.
- Control de accesos al área..
- Conformidad legal.
- Análisis de riesgos.
- Evaluación del plan y los procedimientos de emergencia actuales del departamento y su integración en el plan de contingencia
- Normativas ISO 17799

En el desarrollo de la auditoria informática de seguridad física se aplicó un cuestionario de control interno (Anexo B), del cual se obtuvieron los siguientes resultados:

Las tendencias positivas se orientan a que el 100% de los encuestados admite, que existen: medidas de seguridad en el área física, servicio de vigilancia contratado, adecuación de sistema de aire

acondicionado, se realiza limpieza frecuente a los equipos, copias de seguridad, respaldos, control de acceso a los servidores, licencias etc.

Por otra parte las incidencias negativas se orientan, a la no existencia de vigilancia en el área del departamento de controles de acceso, de extintores, salidas de emergencia, normas de higiene y de seguridad entre otras.

Como puede evidenciarse el control interno en lo que respecta a la seguridad física, es muy débil, puesto que no posen todos los equipos necesarios, ni procedimiento, para contrarrestar cualquier situación de emergencia que se les presente.

Evaluación de riesgos

Descripción/ Riesgos	Error	Desastre Natural	Persona Maliciosa	Persona No Mali.	Mala Infra.	No Ex. Vigilan.	Acceso Libre	Falta Manten.
Destrucción de Hardware	--	2	1	2	2			2
Robo de Hardware	--	--	2	1	2	2	2	--
Pérdidas de Respaldos	2	2	2	1	2	2	2	--
Destrucción del área de Computación	--	2	2	1	2	2	2	--
Uso indebido del Hardware	2	--	2	2	--	--	2	--

Rangos:

1.- Improbable

2.- Probable

Conclusiones

La Seguridad Física de la Dirección de Informática de la UCLA, muestra la no existencia de vigilancia interna a la unidad, para el resguardo de los equipos que allí funcionan, además que se identifican riesgos

potenciales tales como: Destrucción de Hardware, robo de hardware, pérdidas de respaldos, destrucción del área de computación y uso indebido del hardware, lo cuales pueden darse por error, desastre natural, mala infraestructura entre otros.

Asimismo el acceso al área de computación, pueden verse afectado por la ausencia de vigilancia específica para esa área, asi como la falta de controles de acceso, de extintores, salidas de emergencia, normas de higiene y de seguridad etc.

Por otra parte existen medidas de seguridad externas al área física, mediante el servicio de vigilancia contratado, además el área cuenta con adecuado de sistema de aire acondicionado, se realiza limpieza frecuente a los equipos, copias de seguridad, respaldos, control de acceso a los servidores, licencias etc.

Recomendaciones

En cuanto a la Seguridad física, se recomienda seguir las siguientes precauciones básicas:

1. Deben mantenerse en otro lugar, duplicados de todos los archivos, programas y documentación básica.
2. Protección contra excesos de humedad, variaciones de temperatura, caídas de tensión, cortes de suministro, campos magnéticos, actos delictivos, etc.
3. Protección contra incendios, inundaciones, desastres naturales, etc.
4. Plan de emergencia que prevea las actuaciones básicas y medios alternativos disponibles ante distintos niveles de sucesos catastróficos.
5. Designación de un responsable de seguridad y revisión periódica de la operatividad de los medios dispuestos.

6. Seguro que cubra el riesgo de interrupción del negocio y el costo de reconstrucción de ficheros.
7. Diseñar un plan de contingencia que contemple: Actividades antes de un desastre, Actividades durante el desastre y Actividades después del desastre.

4.3. Escenario No. 3:

Tipo de Auditoría Informática: Seguridad Física y Lógica
Empresa: Dirección de Telecomunicaciones de la UCLA.

Programa de Auditoría Informática de Seguridad Física y Lógica aplicado.

- Visita Preliminar
  - Definición del Auditor Líder.
  - Definición de Tipo de Auditoría.
  - Asignación de tareas, actividades y responsabilidades de cada miembro.
  - Definición del alcance de la auditoría.
  - Establecimiento de compromisos por parte de la empresa a ser auditada.
  - Establecer disponibilidad de información de terceros sobre el sistema a ser auditado.
  - Definir plan de visitas e información necesaria.
- Levantamiento de Información
  - Realización de entrevistas.
  - Aplicación de cuestionarios.
  - Investigación sobre manejo del negocio.
  - Investigación del marco legal.

- Desarrollo de la Auditoría
    - Revisión de los documentos, Manuales de usuario y del sistema.
    - Inspecciones y revisiones.
    - Revisión de condiciones de mantenimiento de la infraestructura tecnológica y mantenimiento de procedimientos.
- Revisión y elaboración del informe
    - Discusión grupal y diagnostico de los procesos y el software.
    - Evaluación de hallazgos potenciales.
    - Elaboración de informe.

Una vez realizada la planificación respectiva, se define el alcance de la auditoria informática

Se estableció la Auditoria de Redes para la RedUCLA que está bajo la administración de la Dirección de Telecomunicaciones de la Universidad Centroccidental Lisandro Alvarado (UCLA), y se determinan a continuación los aspectos, características y limitaciones que cubre dicha auditoria, la misma se divide en dos criterios principales como son Auditoria Física, Auditoria Lógica.

En la Auditoría Física, el alcance se limita a: Determinar hasta qué punto las instalaciones físicas de la infraestructura de la UCLA ofrecen garantías internas y externas de acceso y seguridad a la RedUCLA.

En la Auditoría Lógica, el diseño de las redes obedece a una estructura especifica diseñada lógicamente y que se encuentra en diagramas documentados, además de una cantidad de software que están siendo ejecutados, que pueden ser usados indebidamente, estos aspectos que se auditaran específicamente son:

- Contraseñas y procedimientos para limitar accesos no autorizados a la red.
- Monitoreo de la Red.
- Autoridad y responsabilidad del mantenimiento de la Red.
- Controles de importación o exportación de datos.
- Respaldos de las Bases de Datos.
- Cumplimiento de las medidas especificas del espectro electromagnético autorizado por las autoridades pertinentes.

Evaluación del Control Interno:

Se inició el proceso a través de un conjunto de entrevistas al personal de la Dirección de Telecomunicaciones de la UCLA que permiten recopilar información sobre el entorno actual:

- Determinar la existencia de normas que regulen la gestión de la red.
- Seguridad del personal, los datos, *el hardware, el software* y las instalaciones.
- Servicios específicos como Recursos de red, ficheros, correo electrónico, entre otros.
- Revisar si el equipo se utiliza por el personal autorizado e identificar dicho personal.
- Que existan planes para comunicaciones a alta velocidad como fibra óptica, Entro otros.
- Examinar los controles tanto físico como lógicos.

Encuesta a usuarios

La encuesta (Anexo C) se realizó a los usuarios de la RedUCLA, llámense estudiantes, profesores o empleados administrativos, con el fin de obtener información sobre el grado de aceptación, conocimiento y manejo

de los servicios de la Red. A continuación se presentan los resultados obtenidos:

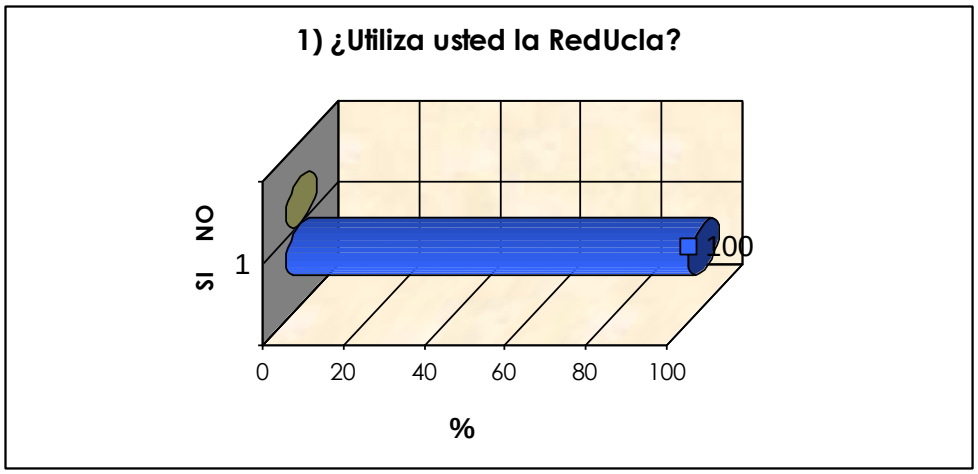


Gráfico No. 1. Uso de la RedUCLA. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

De acuerdo a los resultados obtenidos el 100% de los encuestados opinan que utilizan la RedUcla, por lo que se estima que es un servicio muy necesario para la buena marcha de las actividades académico-administrativas.

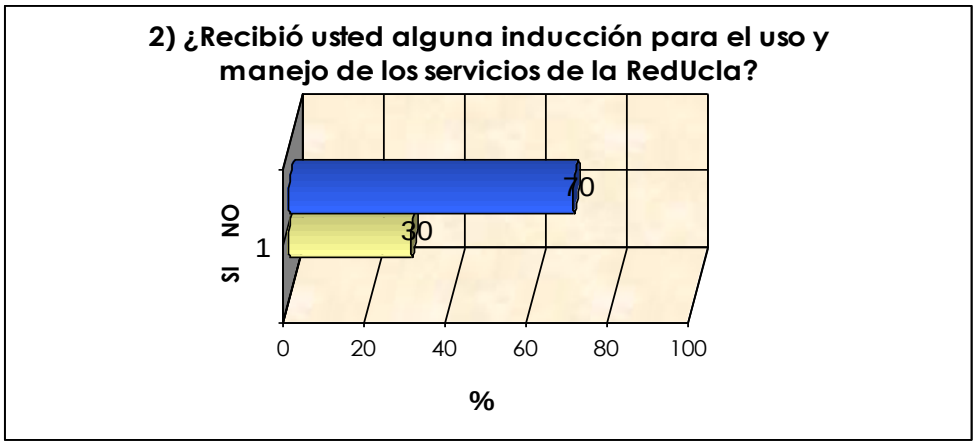


Gráfico No. 2. Inducción para uso y manejo de la RedUCLA. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA . (Anexo C).

Como puede observarse el 70% de los encuestados, dice no haber recibido la inducción necesaria para el uso y manejo de los servicios de la RedUcla, en contraste con el 30% que dice si haber recibido inducción, puede pensarse entonces que el desconocimiento sobre el uso adecuado de los servicios de la RedUcla, puede ocasionar que la misma no se esté utilizando en un estado óptimo.

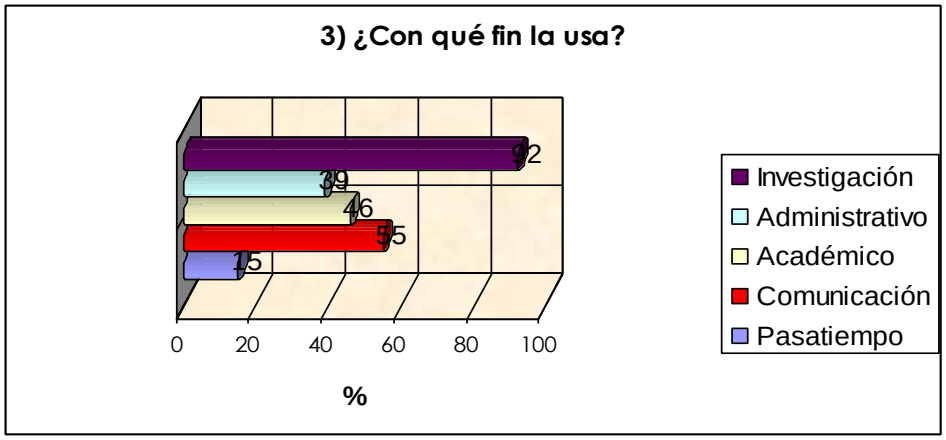


Gráfico No. 3. Fin de uso de la RedUCLA. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

El porcentaje de uso 92% para fines de investigación y 46% para fines académicos, es bastante significativo por lo que se infiere que Reducla debe optimizar los servicios que presta a la investigación y a la académica, tomando en cuenta que son los sectores con mayor demanda de uso de la misma. Por otra parte el sector administrativo que representa el 30%, conlleva al grupo de usuarios que maneja los diferentes sistemas administrativos existentes en la Institución, asimismo el 55% ocupa el fin de uso de comunicación y un 15% dice utilizarlo por pasatiempo. Una vez se puede inferir la necesidad que tiene la RedUcla de optimizar los servicios que presta.

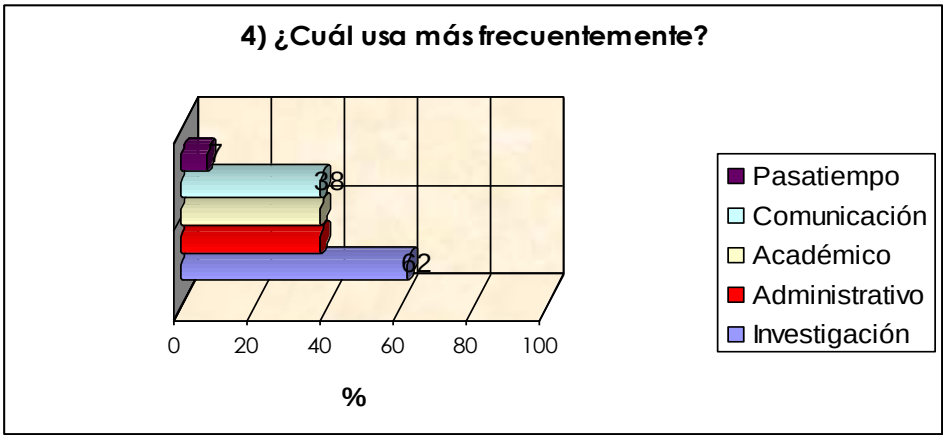


Gráfico No. 4. Frecuencia de Uso de la RedUCLA. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Como puede observarse quienes usan más frecuentemente la RedUcla, son en este orden el 62% investigación, 38% comunicación, académico y administrativo y el 5% pasatiempo, lo cual resulta de gran importancia que la RedUcla optimice los servicios que presta.

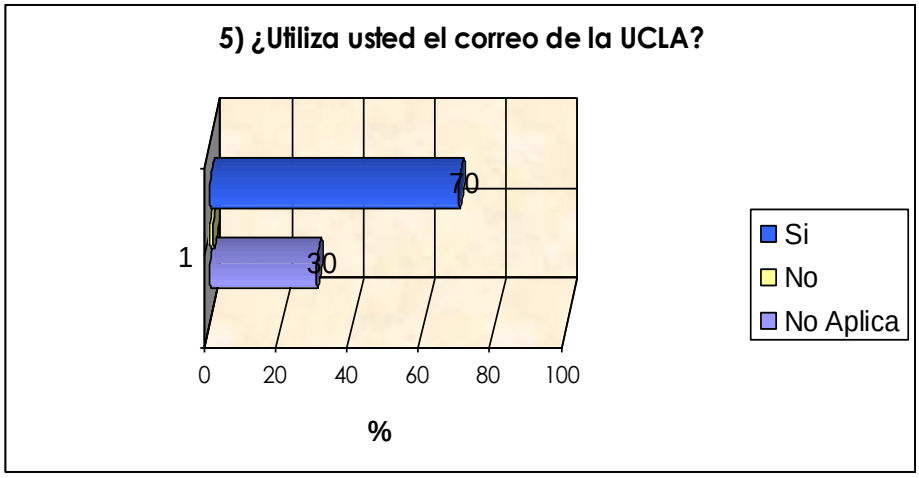


Gráfico No. 5. Utilización del Correo UCLA. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Estos resultados evidencian que el 70% utiliza el correo UCLA y un 30% dice que no es de su interés o utiliza poco el correo, por lo que puede decirse que el uso del correo UCLA, es de gran importancia para los diferentes integrantes que hacen vida en la comunidad universitaria.

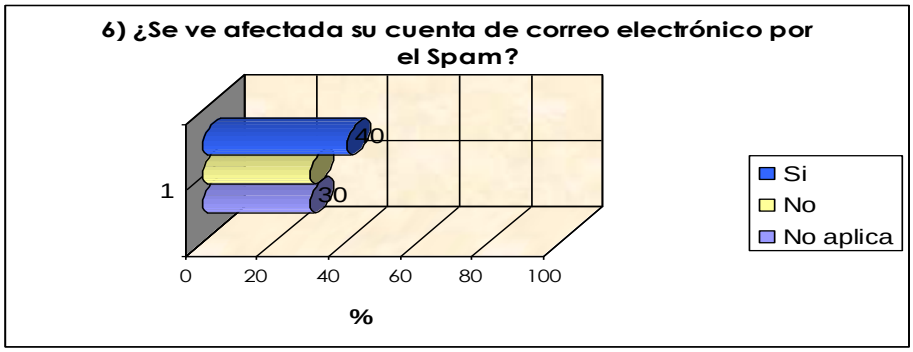


Gráfico No. 6. Cuenta de Correo y Spam. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Estos resultados reflejan que el 40% si ve afectada su cuenta de correo con spam, un 30% dice que no y un 30% no aplica, es decir por este comportamiento se deben tomar correctivos en cuanto al control de spam en las cuentas de correo, por medida obvia de seguridad.

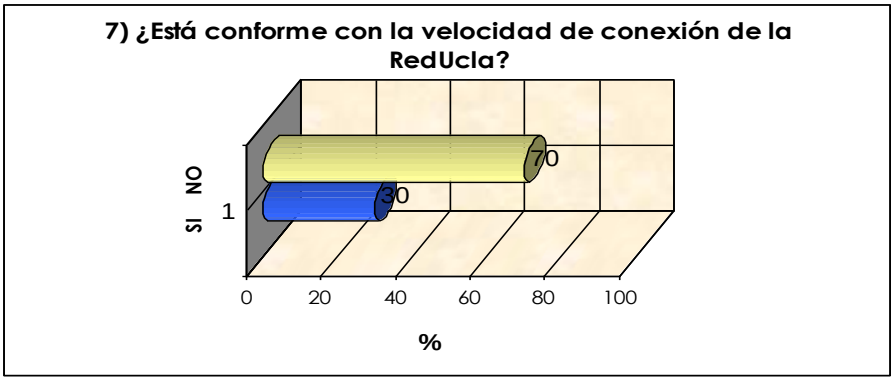


Gráfico No. 7. Velocidad de Conexión. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Se manifiesta un 70% de conformidad en cuanto a la velocidad de conexión y un 30% no lo está, razón por la cual la RedUcla, debe revisar su capacidad instalada, para tener actualizados los equipos que posee y brindar una mejor velocidad de conexión.

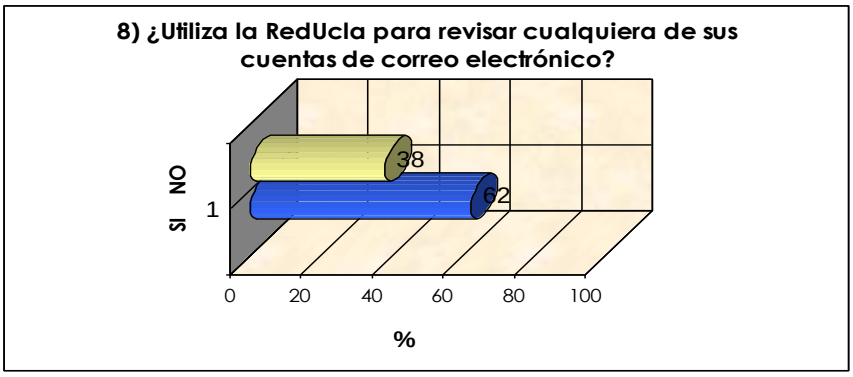


Gráfico No. 8 Cuenta de Correo. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C).

Puede observarse que el 62% revisa otras cuentas de correo electrónico y un 38% dice que no, lo cual a pesar de existir restricciones de uso en algunas páginas electrónicas, existe un porcentaje de usuarios que necesita revisar otras cuentas de correo electrónico, por lo cual deben revisarse las políticas definidas a este respecto.

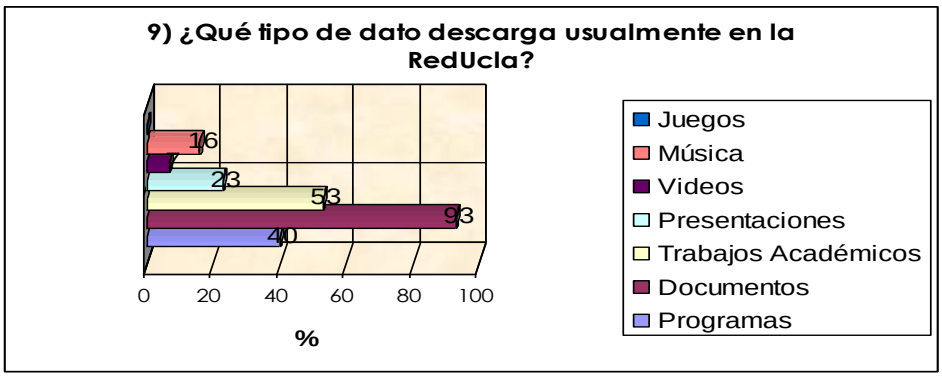


Gráfico No. 9 Tipo de datos que descarga. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Los resultados obtenidos de 93% documentos, 53% trabajos académicos, 40% programas, 23% presentaciones, 16% música y 5% videos, evidencia que los porcentajes más altos, cubren necesidades académicas (documentos, trabajos, programas, presentaciones) el resto en actividades de ocio poco significativas.

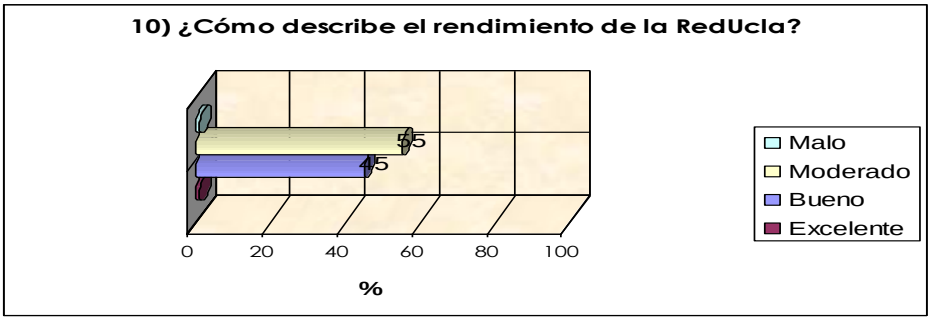


Gráfico No. 10 Rendimiento de RedUcla. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

En cuanto al rendimiento de la RedUcla, el 55% opina que tiene un rendimiento moderado y un 45% opina que es bueno, tomando en cuenta que los resultados obtenidos evidencian que se impone el rendimiento moderado, se infiere que debe evaluarse los equipos y servicios de la Reducla, a fin de optimizar el rendimiento de la misma.

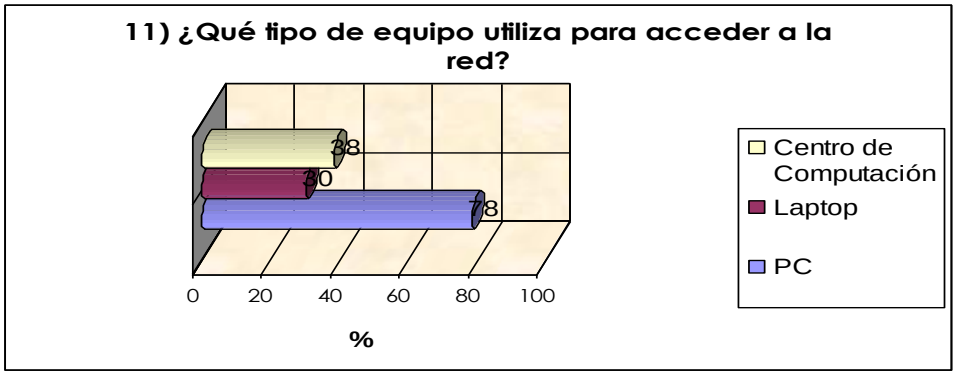


Gráfico No. 11 Cuenta de Correo. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

El 78% utiliza PC, el 38% centro de computación y 30% laptop, lo que evidencia la diversidad de equipos utilizados, razón por la cual la RedUcla debe evaluar constantemente los servicios que presta.

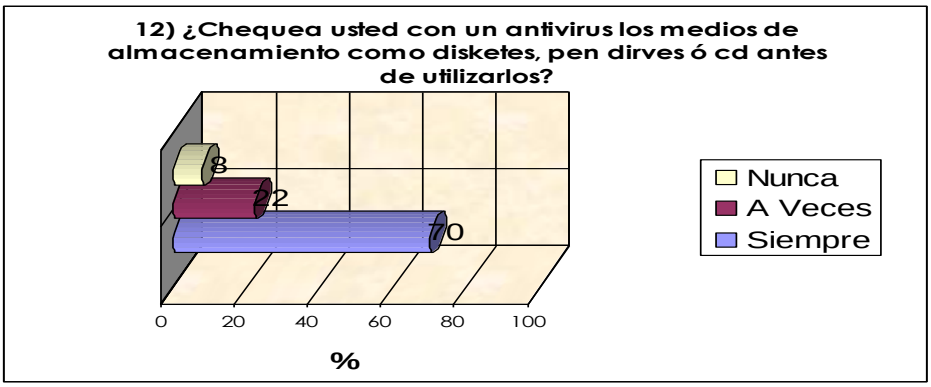


Gráfico No. 12 Utilización del Antivirus. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

En cuanto a la utilización de antivirus, el 70% los usa, el 22% a veces y el 8% nunca los usa, lo cual evidencia la necesidad de crear mecanismos que desarrollen una mayor cultura informática en los usuarios a fin de que utilicen los medios adecuados para la seguridad informática.

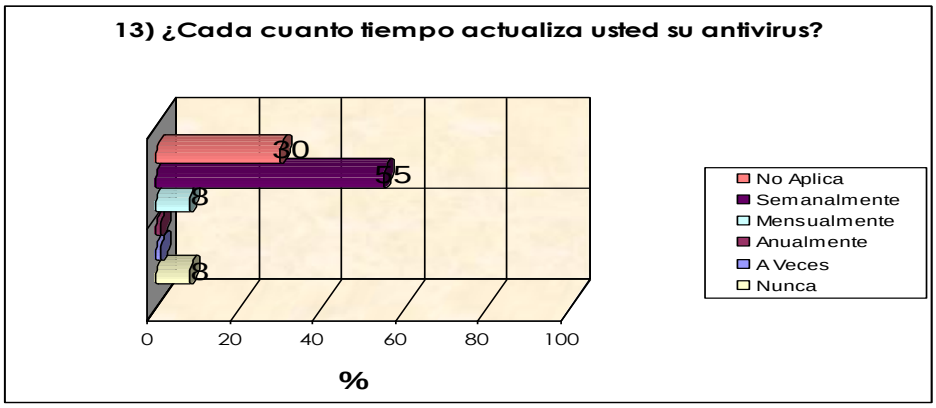


Gráfico No. 13. Tiempo Aplicación del Antivirus. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Al consultar los tiempos de aplicación del antivirus los encuestados opinaron que un 55% lo hace semanalmente, 30% no lo aplica, 18% mensualmente, 18% nunca, 2% anualmente y 2% a veces, lo que indica que en líneas generales algunos usuarios conocen que deben aplicar el antivirus, sin embargo puede decirse que se hace necesario, realizar campañas de concientización a este respecto.

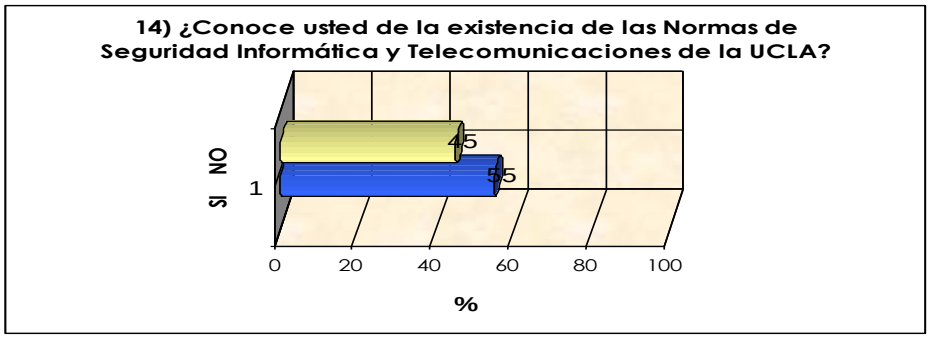


Gráfico No. 14 Normas de Seguridad Informática y Telecomunicaciones. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

El 55% opina que si conoce las Normas de Seguridad Informática y Telecomunicaciones de la UCLA y 45% dice que no las conoce, por lo que se infiere que a pesar de que se conoce la existencia de dichas normas, se hace necesario una mayor divulgación de las mismas.

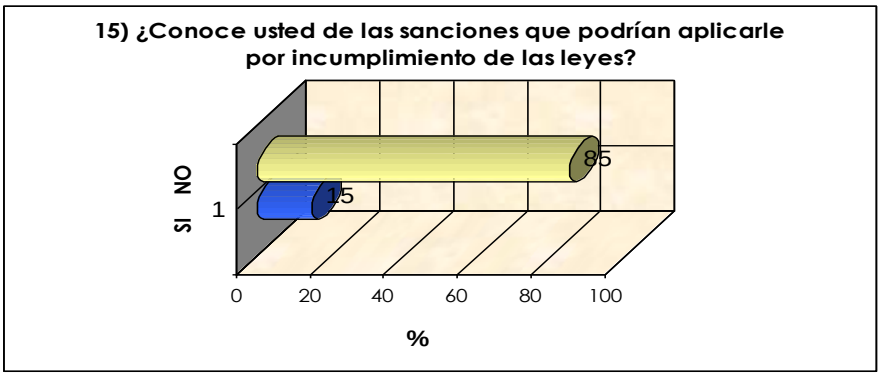


Gráfico No. 15 Sanciones por incumplimiento. Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

Como puede observarse el 15% conoce las sanciones que pueden aplicarse por incumplimiento de las leyes y un 85 % no las conoce, lo cual evidencia la importancia de hacer del conocimiento de los usuarios las sanciones existentes, a los fines de que realicen el uso adecuado de los servicios de las RedUCLA.

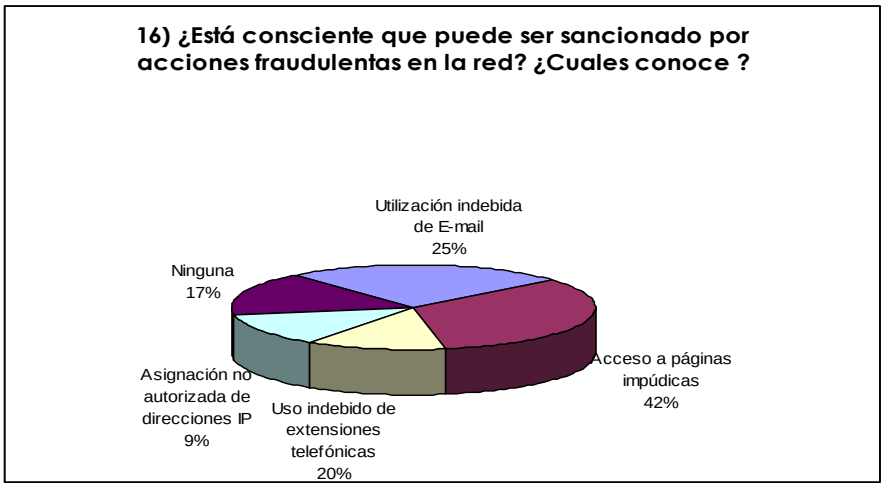


Gráfico No. 16. **Sanciones por acciones fraudulentas.** Resultados de la aplicación del cuestionario de control interno a usuarios de RED-UCLA. (Anexo C)

La mayoría de los usuarios está consciente que puede ser sancionado en un 42% por acceso a páginas impúdicas, 25% por utilización indebida de e-mail, 20% por uso indebido de las extensiones telefónicas, 17% no cree que puede ser sancionado y un 9% por asignación no autorizada de direcciones IP, en este sentido la Dirección de Telecomunicaciones de la UCLA, restringe ciertos accesos, los cuales deben ser comunicados a los diferentes usuarios, a los fines de que se concienticen mas a este respecto.

Matriz de Riesgo:

	CAUSADOS POR TECNOLOGÍA			CAUSADOS POR PERSONAS MAL INTENCIONADAS			OTROS
	Falla en el medio de transmisión	Sobrecarga del tráfico en la red	Disponibilidad de servicios contratados	Hackers en la red	Pinchazos en la red	Virus Informáticos	Errores humanos
Información modificada	I	--	--	P	I	--	P
Información perdida	--	I	--	I	P	P	P
Violación de la privacidad de la Información	--	--	--	P	P	--	--
Datos y/o información Inválida	I	I	--	I	I	I	P
Información no disponible	I	P	P	--	I	--	I

Leyenda:

P: Probable

I: Improbable

Por los resultados obtenidos puede observarse que el personal de la Dirección de Telecomunicaciones opina que los riesgos causados por tecnología (falla en el medio de transmisión) es improbable que ocurra información modificada, datos y/o información inválida e información no disponible, por lo que se infiere que los medios de transmisión poca fallan.

En cuanto a los riesgos causados por tecnología (Sobrecarga del Tráfico en la red) es improbable que ocurra información pérdida y datos y/o información inválida, ya que consideran que no hay sobrecarga del tráfico en la red.

De los riesgos causados por tecnología (Sobrecarga del tráfico de red y disponibilidad de los servicios contratados), opinan que es probable que la información no esté disponible.

Por otra parte en lo que respecta a los riesgos causados por personas malintencionadas (Hackers en la red), es probable que modifiquen

información y violen la privacidad de la misma, pero improbable que la información se pierda o se invalide.

En lo que respecta a los riesgos causados por personas malintencionadas (Pinchazos en la red), es improbable que la información se modifique, se invalide o no esté disponible, pero es probable que se pierda la información y se viole la privacidad de la misma.

Por causa de personas malintencionadas (Virus Informáticos), es probable que se pierda la información e improbable que sea invalidada.

Pueden ocurrir otras situaciones de riesgo por errores humanos, razón por la cual es probable que la información se pierda, se invalide o los datos/información sean invalidados y es improbable que por esta causa la información no esté disponible.

Conclusiones

- Se infiere que el personal se siente parte fundamental y clave de la organización RedUcla razón que hace que su trabajo sea realizado con compromiso y satisfacción. Esto genera una buena gestión, lo cual hace que la RedUcla funcione eficientemente y se mantenga controlada y supervisada.
- Referente a los manuales, falta la aprobación y revisión del Departamento de Organización y Métodos (OyM) y el Consejo Universitario de manera de entrar en Gaceta Oficial vigente.
- Se deduce que la documentación para los procedimientos de contingencia no está realizada para que los preserve en el tiempo de manera que la responsabilidad en cualquier eventualidad no caiga sobre el personal sino sobre el proceso ya probado anteriormente.
- Se verificó que la RedUcla trabaja en el cumplimiento del ancho de banda correspondiente para cada medio de transmisión, la temperatura adecuada para los equipos, las condiciones mínimas ambientales como ausencia de humedad e infiltración y la separación

del cableado de datos/voz con el sistema eléctrico de las instalaciones.

- Se constató que los equipos de comunicación soportan el tráfico de la red por que cuentan con switches Cisco (2960-2959-4000) y routers Cisco (7000) que enrutan y distribuyen el tráfico de la red eficientemente con velocidad de 69Gb.
- El cableado de planta suele ser de cobre (UTP Par Trenzado Categoría 5 y 5e), por lo que es propenso a escuchas ("pinchazos") que pueden no dejar rastros, hasta ahora el Dirección de Telecomunicaciones no ha detectado la existencia de este hecho. Examinando dentro de la red local, el mayor peligro radica en que un usuario de la misma instale una "escucha" no autorizado.
- Se deduce que solo el personal autorizado puede utilizar el software de monitoreo de la red donde se observa el trafico, el acceso a la red, cual equipo esta siendo utilizado y por quien, los puertos utilizados, las aplicaciones de Internet, intercepciones de los mensajes, el funcionamiento de la red, de los segmentos activos, absolutamente todo el control de la red.
- Se identifica que el Departamento de Redes de Datos de la Dirección de Telecomunicaciones lleva un inventario anual de todos equipos hardware incluyendo tarjetas de red, PC's, impresoras, switches, routers, cableado, servidores, UPS, entre otros. Es un trabajo extenso pero bien riguroso que se realiza para que no se manipulen indebidamente los equipos o se extravíe alguno, debido que la RedUcla pertenece a una organización pública y debe rendir cuentas de sus activos.
- Se observó que en la RedUcla se cuenta con una base de datos extensa de todos los usuarios que pueden acceder a la red para garantizar su seguridad, sin embargo destacamos que el peligro mas

frecuente es que un extraño se introduzca desde el exterior hasta la red interna.

- Se verificó que existen políticas de protección como firewall donde se autoriza específicamente ciertos servicios especiales, por ejemplo, correo electrónico e Internet para todos los usuarios y otros servicios a usuarios específicos, así como también se restringen aplicaciones que no cumplen ningún objetivo académico y solo consumen ancho de banda.
- Se infiere que en la instalación de programas y aplicaciones, cada usuario personaliza su computador, esto es una debilidad de la red porque debería existir un control de las utilidades requeridas por cada usuario.
- En cuanto a la seguridad de la información es importante destacar que los ficheros, mensajes y contraseñas que viajan por la RedUcla son cifrados pero las aplicaciones que se ejecutan en cada equipo son independientes, y no se cifran, podemos mencionar la más obvia: el uso de Internet, allí la información es de dominio público y cualquiera la puede interceptar, usurpar, modificar, duplicar o ver con un simple software.

Recomendaciones.

1. Solicitar apoyo al Decanato de Ciencias y Tecnología, que ejecute alguna actividad donde se seleccione alumnos capacitados, con conocimientos en redes, para que contribuyan en la realización de la documentación que falta en la Dirección de Telecomunicaciones.
2. Se aconseja el desarrollo de la documentación de los procedimientos de contingencia. Además la implementación de servidores MIRROR que mantenga información duplicada en caso de fallas como por ejemplo la caída del servidor de correos.(MIRROR es un término usado en Internet para hacer

referencia a un servidor FTP, página WEB o cualquier otro recurso que es espejo de otro).

3. Motivar el cumplimiento de las Normas de Seguridad Informática y Telecomunicaciones de la UCLA. Una propuesta seria realizar foros para informar a los usuarios de los riesgos, realizar un resumen con los artículos más resaltantes y suministrárselos por escrito a los usuarios, la idea es garantizar que la información llegue a ellos y se interesen por leerla.
4. Se aconseja disminuir la temperatura (-grados) del recinto donde están los servidores principales de la red agregándole mejor acondicionamiento a los equipos, para que no se recalienten.
5. Es imprescindible tener un control estricto de los equipos de escucha bien sea físicos (“sniffer”) y lógicos (traceadores) ambos escuchadores, son de uso habitual, por lo tanto es fundamental que ese uso sea legitimo y exista el monitoreo constante de la red que no devenga una actividad espuria.
6. Instalar un Firewall IDS que se encargue de prevenir y controlar el tráfico de datos no autorizado entre las redes conectadas a la RedUcla.
7. Es vital vigilar y controlar el acceso a los software de monitoreo, ya que el uso y movimiento de esta información en manos oscuras puede ser contraproducente para la Red.
8. Se recomienda, realizar una base de datos con información de los equipos de la red, donde se incluyan los movimientos de los equipos y las inclusiones de los nuevos, de manera de mantener actualizada la información del inventario.
9. Es aconsejable por medidas de seguridad, probar periódica, controlada y preventivamente que se intenten saltar los procedimientos de seguridad; antes de que un extraño los ponga a prueba para acceder a la Intranet o la Extranet.

4.4. Escenario No. 4:

Tipo de Auditoría Informática: Seguridad

Empresa: Centro de Computación del Decanato de Ciencias y Tecnología de la UCLA

Programa de Auditoría Informática de Seguridad aplicado.

- Visita Preliminar
  - Definición del Auditor Líder.
  - Definición de Tipo de Auditoría.
  - Asignación de tareas, actividades y responsabilidades de cada miembro.
  - Definición del alcance de la auditoría.
  - Establecimiento de compromisos por parte de la empresa a ser auditada.
  - Establecer disponibilidad de información de terceros sobre el sistema a ser auditado.
  - Definir plan de visitas e información necesaria.
- Levantamiento de Información
  - Realización de entrevistas.
  - Realización de cuestionarios.
  - Investigación sobre manejo del negocio
  - Investigación del marco legal.
- Desarrollo de la Auditoría
  - Revisión de los documentos, manuales de usuario y del sistema.
  - Inspecciones y revisiones.
  - Revisión de condiciones de mantenimiento de la infraestructura tecnológica y mantenimiento de procedimientos.
- Revisión y Elaboración del Informe

- Discusión grupal y diagnostico de los procesos y el software.
- Evaluación de hallazgos potenciales
- Elaboración del informe.

Una vez realizada la planificación respectiva, se define el alcance de la auditoria informática

El estudio, desarrollo y aplicación de la Auditoria de Seguridad Informática, se enfoco hacia algunos aspectos de los procesos lógicos y físicos en el área del Centro de Computación del Decanato de Ciencias y Tecnología de la UCLA.

Evaluación del Control Interno:

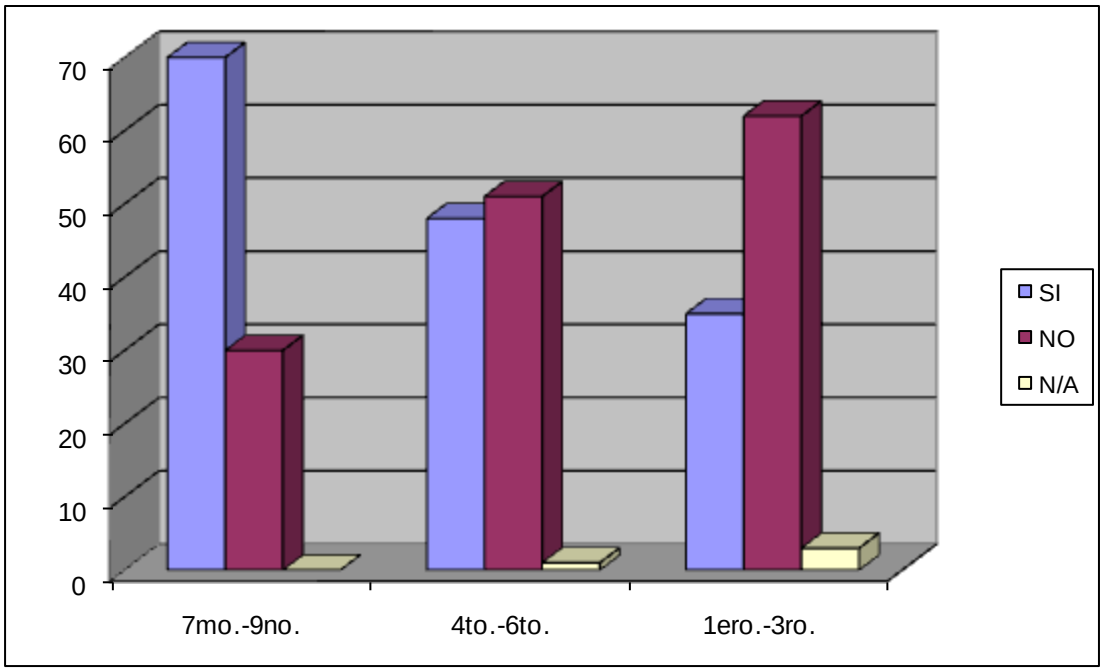
En la visita preliminar se solicitó a la encargada del Centro de Computación del DCyT documentos de sistema y de la organización tales como:

- Políticas, estándares, normas y procedimientos
- Organigrama
- Manuales
- Planes de Seguridad
- Inventario (software y equipos)
- Planes de Contingencia.

Se aplicó un cuestionario, dirigido a estudiantes (usuarios) (anexo D) y otro a preparadores y personal ayudante de soporte técnico (anexo E).

Dimensión controles, normas y políticas de seguridad

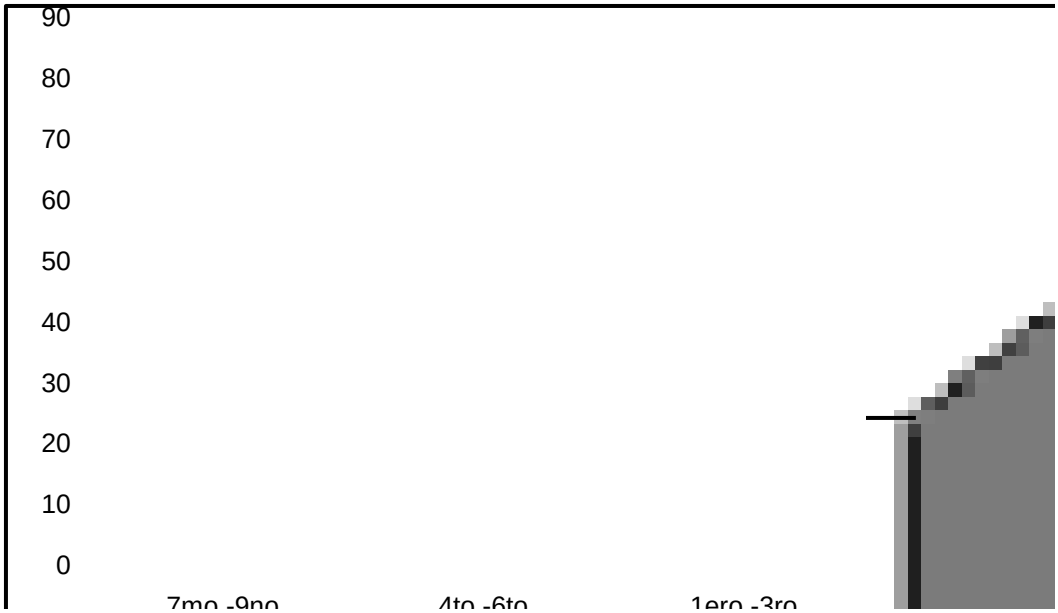
¿Conoce las normas y reglamentación de uso de las áreas y los equipos informáticos?



Fuente: Instrumento aplicado a estudiantes (anexo D)

Como puede observarse el comportamiento sobre el conocimiento de normas y reglamentos por los usuarios del centro de computación, se da en el siguiente orden 70% (7mo-9no.), 51% (4to.-6to) y 62% (1ero-3ro), porcentajes que representan el Si conocen dichas normas y reglamento. Por otra parte, 30% (7mo-9no.), 48% (4to.-6to), 35% (1ero-3ro) y 1% (4to-6to.), 3% (1ero-3ro), manifiestan no conocer las mismas, en tal sentido puede inferirse, la necesidad de hacer una mayor divulgación de las normas y reglamentos en materia de seguridad.

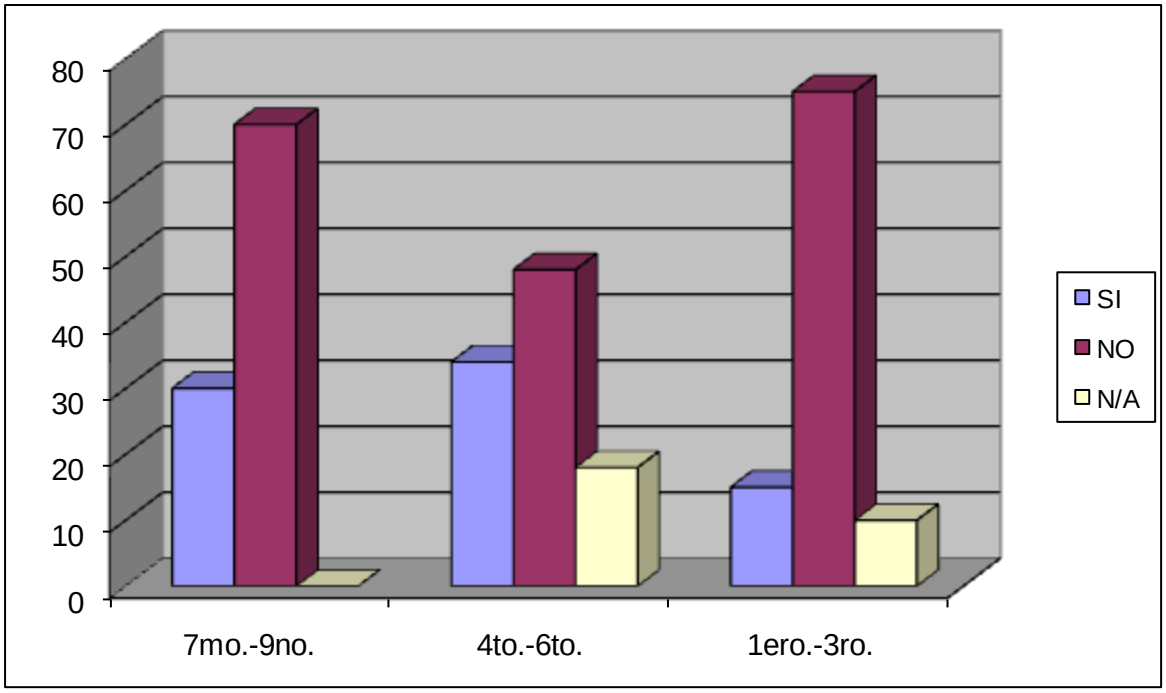
¿Considera que el software y las políticas de seguridad vigentes son suficientes para garantizar la protección e integridad de los equipos?



Fuente: Instrumento aplicado a estudiantes (anexo D)

De los resultados obtenidos, puede observarse que el 87% (7mo-9no.), 70% (4to.-6to) y 58% (1ero-3ro), consideran que no es suficiente el software y las políticas de seguridad vigentes para garantizar la protección e integridad de los equipos, el 13% (7mo-9no.), 18% (4to.-6to), 12% (1ero-3ro) y 12% (4to.-6to) y 30% (1ero-3ro), opinan que sin son suficientes y el resto piensa que no tiene respuesta a este respecto, puede decirse que se hace necesario evaluar el software y las políticas de seguridad vigentes para garantizar la protección e integridad de los equipos, actualmente existentes, a fin de realizar los ajustes necesarios para la seguridad de los mismos.

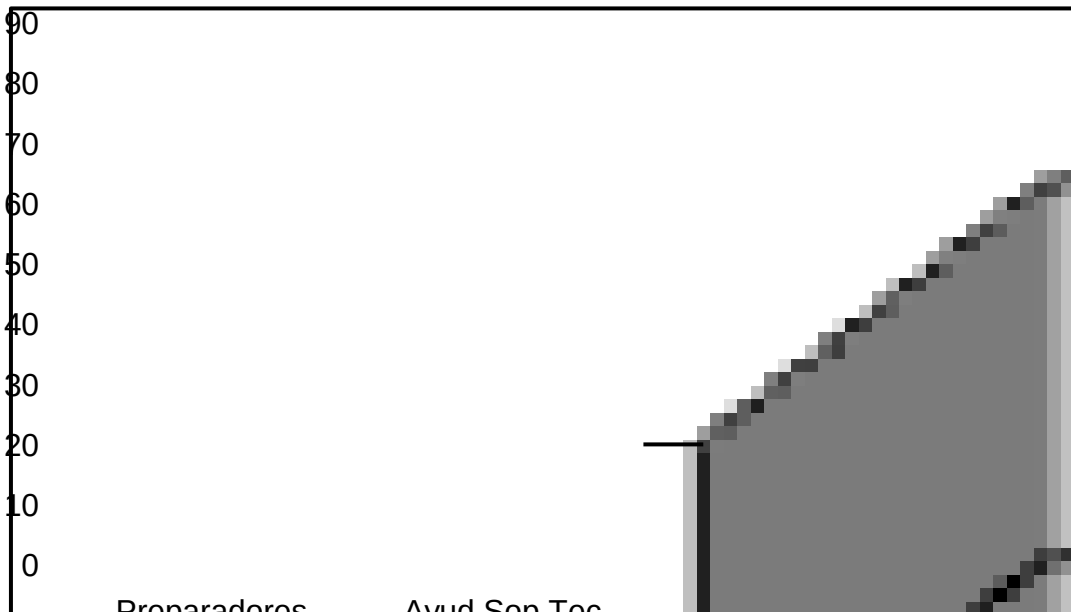
¿Existe difusión de las normas y políticas de seguridad del Centro de Computación?



Fuente: Instrumento aplicado a estudiantes (anexo D)

Puede observase que es notorio que el 70% (7mo-9no.), 48% (4to.-6to) y 75% (1ero-3ro), opina que no existe difusión de las normas y políticas de seguridad del Centro de Computación, además el 30% (7mo-9no.), 34% (4to.-6to), 15% (1ero-3ro) y el 18% (4to.-6to) y 10% (1ero-3ro), estiman que si existe difusión de las normas y políticas de seguridad y el resto no opina al respecto. En el presente análisis se corrobora que es mayor el porcentaje de usuario(a)s que opina que no existe difusión, por tanto deben tomarse los correctivos necesarios

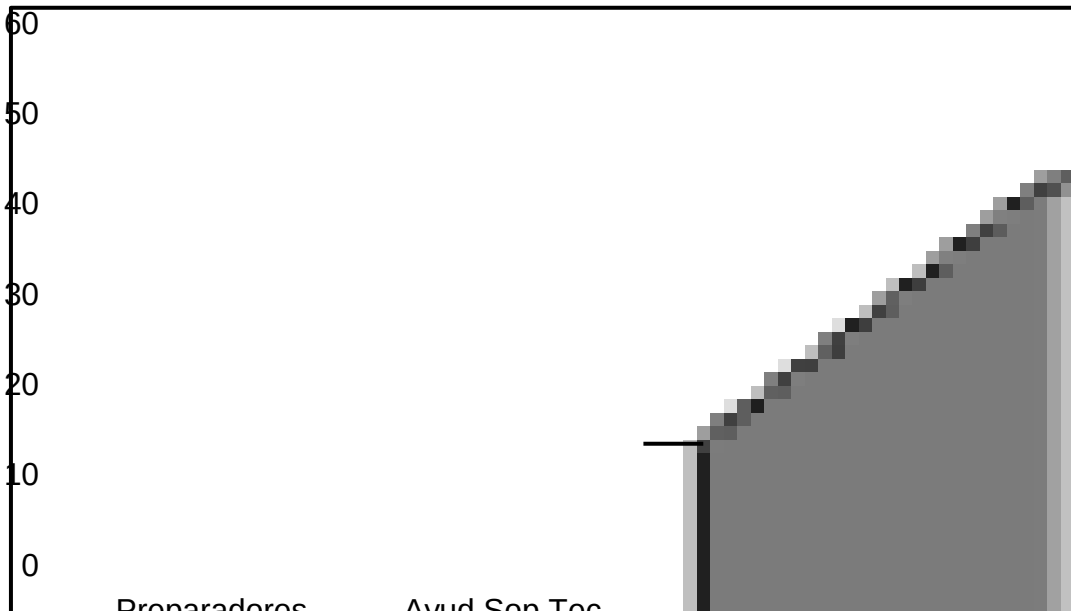
¿Conoce reglamentación y políticas de seguridad para laborar en CCDCYT?



Fuente: Instrumento aplicado a preparadores y Ayudantes de Soporte Técnico del CCDCYT (anexo E)

Al entrevistar a los preparadores y ayudantes de soporte técnico del Centro de Computación del DCyT, 90% y 85% respectivamente opinan que si conoce la reglamentación y políticas se seguridad para laborar en CCDCYT y el 10% y 5 %, dice que no y un 10% no opina al respecto, puede decirse que a pesar de que existe conocimiento entre preparadores y ayudantes de soporte técnico de la normativa existente, se debe lograr que todos conozcan de las mismas.

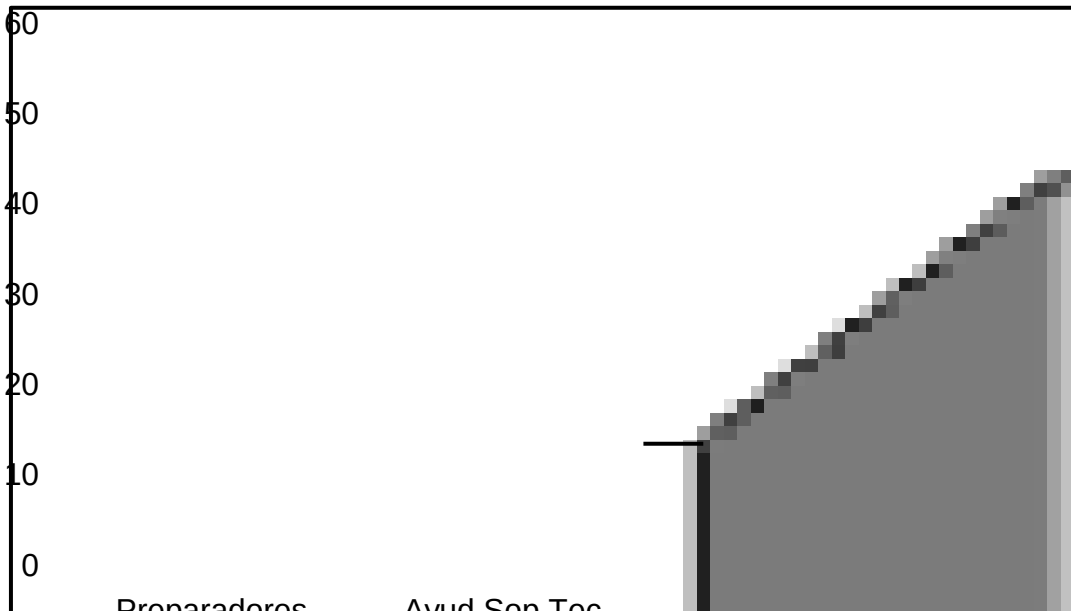
¿Existe difusión de las normas y políticas de seguridad del Centro de Computación?



Fuente: Instrumento aplicado a preparadores y Ayudantes de Soporte Técnico del CCDCYT (anexo E)

A este respecto los preparadores y ayudantes de soporte técnico, opinan en un 60% y 57%, que no existe difusión de las políticas y normas de seguridad del CCDCYT y el 40% y 33% afirma que si hay difusión de las mismas, por lo que se insiste en que deben tomarse medidas para ampliar el proceso de difusión de las políticas y normas de seguridad informática.

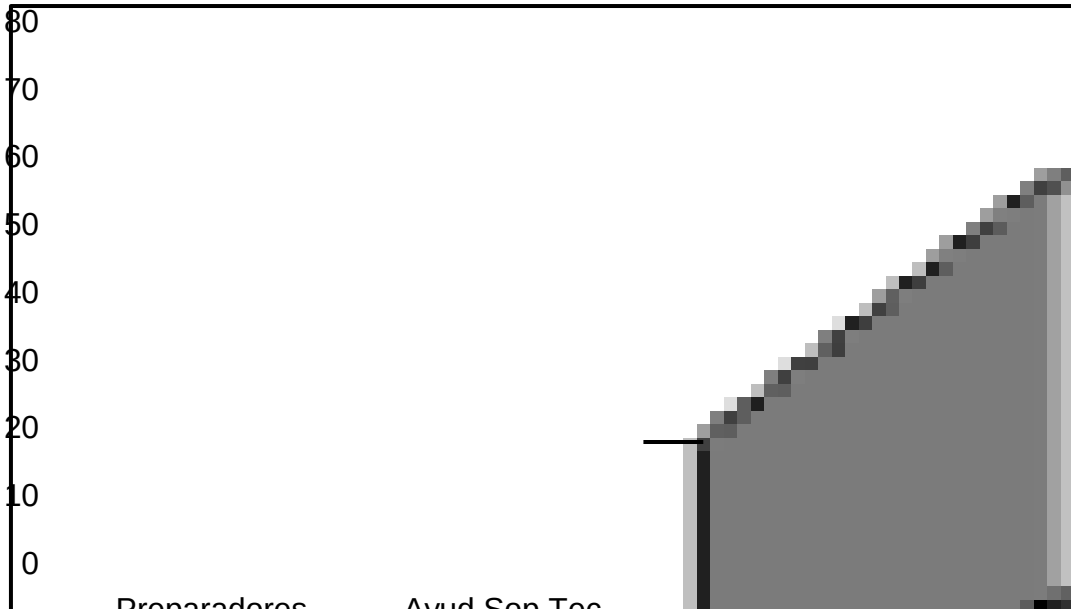
¿Cree que los controles de acceso al sistema y a los recursos informáticos; son suficientes para evitar intrusiones, daños o actividades no autorizadas?



Fuente: Instrumento aplicado a preparadores y Ayudantes de Soporte Técnico del CCDCYT (anexo E)

De los resultados obtenidos se observa que los preparadores y ayudantes de soporte técnico de CCDCYT, opinan en un 60% y 57%, que los controles de acceso al sistema y a los recursos informáticos, no son suficientes para evitar intrusiones, daños o actividades no autorizadas, el 40% y 29%, opina que si y el 14% no opina al respecto, puede inferirse entonces que se hace necesario evaluar los controles y recursos informáticos actualmente existentes, para contribuir con la seguridad que se requiere.

¿Considera que los mecanismos y controles de seguridad implantados en el CCDCYT avalan la confidencialidad e integridad de la información, así como la protección de los equipos?



Fuente: Instrumento aplicado a preparadores y Ayudantes de Soporte Técnico del CCDCYT (anexo E)

En lo que respecta a la consulta sobre si considera que los mecanismos y controles de seguridad implantados en el CCDCYT avalan la confidencialidad e integridad de la información, así como la protección de los equipos, los preparadores y ayudantes de soporte técnico, opinan en 80% y 57% que no son suficientes los mecanismos actualmente existentes y un 20% y 43% opina que si, por lo que se recomienda revisar los mecanismos existentes.

ANALISIS FODA BASADO EN CUESTIONARIOS REALIZADOS A USUARIOS DEL CENTRO DE COMPUTACIÓN DEL DCYT (CCDCYT)

Fortalezas

Estudiantes que cursan el 7mo. al 9no. Semestre de la carrera de ingeniería informática, hay fortaleza solamente en el conocimiento de las normas y reglamentación de uso de las áreas y los equipos informáticos. Esta fortaleza se debe a que los estudiantes de semestres avanzados, ya han usado el CCDCYT para cumplir con las exigencias de la carrera, pero no es porque existe difusión de las mismas.

Debilidades

Se observa debilidad en las normas que garantizan el buen funcionamiento de los equipos y dispositivos informáticos, dado que en el reglamento existente no ofrece una adecuada protección a los equipos, un procedimiento que garantice la eficiencia del software seguridad instalado, en las políticas de seguridad implementadas para el uso de las áreas y protección e integridad de los equipos y en la difusión de las normas de políticas de seguridad del CCDCYT.

Oportunidad

Entre las oportunidades que se presentan para mejorar el funcionamiento de las áreas del CCDCYT y garantizar la seguridad e integridad de los equipos informáticos y el software instalado, se mencionan las siguientes:

- Publicar en los medios disponibles (carteleras) las normas y reglas para el uso de las áreas y los equipos informáticos y así garantizar la difusión de las mismas.

- Establecer normas y reglas para lograr un buen funcionamiento y la protección de los equipos y dispositivos informáticos.
- Implantar un software (antivirus, firewalls) eficiente para aumentar la seguridad del sistema.
- Mejorar la distribución de los equipos instalados en las áreas para su mayor seguridad.
- Garantizar que los usuarios cumplan con las reglas y normas establecidas.

Amenazas

Entre las amenazas que se observaron y que afectan el funcionamiento de las áreas del CCDCYT y la seguridad e integridad de los equipos informáticos y el software instalado están:

- Mal funcionamiento de equipos y dispositivos informáticos a causa del mal uso de los mismos, por parte de los usuarios debido a desconocimiento y a la no difusión de las normas y políticas de seguridad, además de no contar con software adecuado para la protección e integridad del sistema.
- Pérdida parcial o total de equipos y dispositivos físicos en caso de desastre por la falta de mecanismos físicos de seguridad y planes contingencia.
- Interferencia o pérdida de información ya que no se cuenta con medios para respaldar la misma, ni con claves de acceso que restrinjan de manera segura el sistema.
- Robo y/o hurto de equipos a consecuencia del no cumplimiento de normas de acceso a los laboratorios.

- Desacato a las normas y políticas de seguridad por no contar con personal dedicado a la seguridad informática, viendo a esta como una función aislada y no como un elemento vivo de la organización.

4.5. Escenario No. 5:

Tipo de Auditoría Informática: Organización y Métodos

Empresa: Barreto Seguros C. A.

La auditoria de organización y métodos de la empresa se enmarca en el estudio de los manuales existentes, los procesos que se realizan y los usuarios involucrados en dichos procesos.

Objetivo General

Evaluar el nivel de sistematización de los procesos descritos en los manuales existentes en la organización.

Objetivos Específicos

1. Contrastar la ejecución de los procesos con lo que está definido en los manuales de la organización
2. Determinar la existencia de Sistemas de Información que faciliten el cumplimiento de los objetivos empresariales.
3. Determinar el conocimiento de los usuarios acerca de la información existente en los manuales.

Hallazgos de la Auditoria Informática de Organización y Métodos:

Dimensiones e Indicadores de los Objetivos Específicos

Objetivo 1

Contrastar la ejecución de los procesos con lo que está definido en los manuales de la organización:

Dimensión	**Indicadores**	**Cuestionario**
Manuales	– Ubicación. – Accesibilidad. – Responsable.	– ¿Dónde se encuentran? – ¿Quiénes tienen acceso a los manuales? – ¿Quién posee los manuales?
Proceso	– Responsabilidad. – Duración. – Ejecución. – Conveniencia. – Sistematización.	– ¿Quién es el responsable del proceso? – ¿Cuánto dura el proceso en realizarse? – ¿Cuándo se realiza el proceso? – ¿Se hace el proceso en el momento adecuado?
Usuario	– Capacitación.	– ¿Están los usuarios

	– Eficacia. – Eficiencia. – Disponibilidad.	capacitados para realizar el proceso? – ¿Los usuarios cumplen con los objetivos del proceso? – ¿Los usuarios usan los recursos de forma adecuada? – ¿La carga horaria asignada al responsable es suficiente para realizar el proceso de forma exitosa?
Controles	– Existencia. – Cumplimiento. – Supervisión. – Frecuencia.	– ¿Existen controles internos para la ejecución del proceso? – ¿Se cumplen los controles? – ¿Con qué frecuencia se aplican? – ¿Existe alguien que supervise el cumplimento de dichos controles?
Marco Legal	– Existencia.	– ¿Existe un Marco

	– Cumplimiento. – Supervisión.	Legal por el cual se rija la sistematización de los procesos?. – ¿Se cumple lo establecido en el Marco Legal?. – ¿Quién vela por el cumplimiento?.

Objetivo 2

Determinar la existencia de Sistemas de Información que faciliten el cumplimiento de los objetivos empresariales.

Dimensión	Indicadores	Cuestionario
Sistemas	– Existencia – Cantidad – Tipo	– ¿Existen Sistemas de Información en la empresa? – ¿Cuántos hay? – ¿Qué tipo de sistemas son?
Manuales	– Existencia – Accesibilidad	– ¿Existen manuales para adiestrar a los usuarios en el uso de esos sistemas? – ¿El usuario tiene acceso siempre a los manuales?
Satisfacción	– Logro de	– ¿Los sistemas

	Objetivos	satisfacen las necesidades de la empresa?

Objetivo 3

Determinar el conocimiento de los usuarios acerca de la información existente en los manuales.

Dimensión	Indicadores	Cuestionario
Preparación	– Capacitación. – Tipo. – Duración.	– ¿Se le da capacitación al usuario con la información de los manuales? – ¿Qué tipo de capacitación se le da? – ¿Cuánto tiempo dura?
Manuales	– Accesibilidad.	– ¿El usuario tiene acceso siempre a los manuales?
Conocimiento	– Nivel de preparación. – Supervisión. – Recapacitación.	– ¿El usuario fue capacitado? – ¿Se evalúa el conocimiento de los manuales? – ¿Se recapacitan los usuarios?

Hallazgos

Es importante destacar que para este escenario, solo se realizó revisión de manuales del área de producción y conversaciones informales con algunos trabajadores de la Empresa, por lo que el alcance y las recomendaciones son limitadas.

Al revisar los papeles de trabajo aparentemente están presentes los siguientes hallazgos:

- No se cuenta con un sistema de información en el área producción que permita tener registrada la información de forma veraz.
- Los empleados que están involucrados en el área de corte de láminas corren un riesgo mayor de enfermedades de vías respiratorias debido a la falta de protección.
- Se desperdicia materia prima a la hora de cortar las piezas tal y como vienen en la orden.
- Se pierde dinero pues no se verifica que las bóvedas estén bien hechas antes de pasarlas al área de instalación, lo que trae como consecuencia el deterioro de la pintura y/o la alfombra a la hora de corregir el desperfecto.
- No existen controles que impidan la entrada al taller de personas no autorizadas.

Conclusiones y Recomendaciones

Luego de la realización de la auditoría podemos concluir que la sistematización dentro de la empresa es aceptable para ejecutar las tares administrativas básicas, sin embargo, es necesario buscar una solución automatizada que sea capaz de satisfacer todas las necesidades de proyección que se tienen.

El proceso de elaboración de bóvedas de seguridad tal y como se realiza actualmente cumple con la mayoría de los objetivos organizacionales de la empresa pues es capaz de producir lo necesario para satisfacer las necesidades de los clientes actuales, además el proceso es bastante similar al descrito en el manual salvo por algunos detalles de seguridad de los empleados. Sin embargo la ausencia de la automatización en ésta parte fundamental de la empresa le impide crecer a un ritmo más acelerado, exige un mayor esfuerzo por parte de los empleados y trae como consecuencia el aumento del tiempo de espera por parte de los clientes para conseguir el producto. Es recomendable entonces optimizar el tiempo de entrega, el costo, las ganancias y la seguridad de los empleados a la hora de realizar dichas bóvedas.

Para lograr lo planteado anteriormente se recomiendan las siguientes acciones:

- Usar un sistema que permita digitalizar los moldes de las bóvedas y cortarlos automáticamente. de ésta manera se ahorra espacio y se disminuyen errores humanos a la hora de cortar.
- Hacer un estudio que determine si es factible reemplazar el sistema administrativo o realizar modificaciones al ya existente.
- Aislar el área de cortado de las demás para evitar la exposición de los empleados al humo.
- Crear una clasificación de los vehículos de acuerdo al tamaño, que permita tener láminas para cada clasificación de tal forma que sea posible acomodar la mayor cantidad de cortes en la lámina para lograr minimizar el desperdicio de materia prima.

- Colocar un punto de control después de soldar las últimas piezas para asegurar que la lamina está bien doblada y las demás piezas estén bien soldadas, con esto se evitan perdidas de dinero ya que es posible corregir antes de pintar y colocar la alfombra.
- Contratar una persona que se encargue de supervisar todas los técnicos del taller y darle llaves solo a el, de esta forma se sabe con certeza quien entra y sale del área de producción.

4.6. Escenario No. 6:

Tipo de Auditoría Informática: Mantenimiento SISTEMAS CONSEDE – DIM UCLA

Empresa: Departamento de Mantenimiento de la UCLA.

Programa de Auditoría informática de mantenimiento aplicado

- Definición de Objetivos y Alcance
  - Reunión de Equipo de Auditoría
  - Elaboración de Instrumentos de Medición.
  - Establecer lineamientos para levantamiento de información.
  - Estudio y discusión del alcance de la auditoría.
- Recopilación de Información
  - Levantamiento de información acerca de Bases de Datos del sistema.
  - Reunión de Equipo de Auditoría.
  - Perfeccionamiento de Instrumentos de medición.
  - Visita Dirección de Mantenimiento de la UCLA.
  - Reunión con usuarios de CONSEDE.

- Identificación de Controles de Seguridad en Base de Datos.
- Revisión de Control Interno.
- Información acerca de historia del sistema y problemática presentada.
- Análisis de información recolectada.
- Desarrollo y perfeccionamiento de la estrategia de auditoría.

– Ejecución del Programa de Trabajo
  - Reunión Equipo de Auditoría: Análisis de material obtenido.
  - Visita a Mantenimiento Núcleo Central - Usuarios de DIM UCLA.
  - Visita a Mantenimiento Núcleo Obelisco – Usuarios DIM UCLA y CONEDE.
  - Identificación de Controles en Seguridad de Base de Datos.
  - Especificación de Hallazgos. Estudio de procesos en CONEDE Y DIM UCLA.
– Identificación de controles y riesgos
  - Gestión de riesgos latentes del sistema.
  - Análisis de frecuencias e impacto.
  - Análisis de controles aplicados y a sugerir para CONSEDE y DIM UCLA.
– Revisión y Elaboración del Informe
  - Discusión grupal y diagnostico de los procesos y funcionalidades.
  - Evaluación de hallazgos potenciales

- Elaboración del informe.

Ejecución de la auditoría

- Se comenzó con el estudio, discusión y definición del alcance y objetivos de la auditoria, se revisó información relacionada con auditoría de base de datos realizada anteriormente.
- Discusión sobre la información recolectada, nueva revisión e identificación de riesgos potenciales.
- Visita al Departamento de Mantenimiento UCLA Se identificaron los Controles de Seguridad en Base de Datos. Revisión de Control Interno. Se logró un conocimiento general de las funciones de CONSEDE y DIM UCLA.
- Información acerca de historia del sistema, antecedentes del sistema y problemática presentada.
- Análisis de información recolectada en visita y elaboración de informe sobre realidad presentada con el sistema CONSEDE.
- Diseño y definición de una nueva estrategia de auditoría, motivada por la problemática existente con los sistemas CONSEDE y DIM UCLA, redefinición de objetivos de auditoría.
- Nueva visita al Departamento de Mantenimiento UCLA en esta oportunidad la visita estuvo destinada a la realización de pruebas de caja negra para verificar la existencia de controles de seguridad identificados en la visita anterior
- Visita a la Sección de Mantenimiento Núcleo Central Identificación de controles de seguridad establecidos para la

base de datos y realización de pruebas de caja negra a dichos controles. Estudio de procesos de CONSEDE y DIM UCLA.

- Visita a la Sección de Mantenimiento Núcleo Obelisco, Conocimiento del funcionamiento general del sistema DIM UCLA en la sede correspondiente al Núcleo Obelisco.
- Identificación de debilidades del sistema.
- Se realizó entrevista a los encargados de Dirección de Mantenimiento, Sección Central y Sección Núcleo Obelisco respectivamente.
- De la información recolectada en las visitas (sede del Departamento de Mantenimiento, sede Central, sede Núcleo Obelisco), así como de las entrevistas realizadas se hizo análisis Definiendo controles para CONSEDE y DIM UCLA, bajo la clasificación: preventivos, de detección y correctivos.

Elaboración de matriz de riesgos

De las respuestas obtenidas en las entrevistas así como el análisis de las funcionalidades de sistema CONSEDE y DIM UCLA, se puede decir que el mismo presenta deficiencias en su funcionalidad y su seguridad es altamente vulnerablemente, debido a la escasa existencia de controles de seguridad en elementos primordiales como controles de acceso (tanto al sistema como a la base de datos), estándares para la creación de nombres de usuario y claves, registro de actividades de usuario, etc. Seguidamente, se presenta la matriz de riesgos.

RIESGO INHERENTE	IMPACTO
Daño de los archivos contentivos de la arquitectura de datos del sistema debido a virus, manipulación errónea de los mismos, fallas eléctricas, entre otros fenómenos.	3
Acceso indebido a la base de datos por parte de usuarios no autorizados.	2
Carga, modificación, eliminación y gestión de reportes directamente a la base de datos, sin uso del sistema.	2
Inconsistencia de datos derivada de registros erróneos, incompletos.	3
Pérdida de datos históricos debida a ausencia de una gestión de respaldos.	3
Falla de conexión entre núcleos UCLA para control de actividades y generación de reportes.	3
Generación de reportes de OT, SS y TP con información incompleta o poco significativa.	3
Uso de la información con fines desconocidos por parte de terceros.	3
Incompatibilidad de versiones en sistemas operativos y manejador de base de datos a de migrar a otras versiones.	3
Colapso del sistema por obsolescencia tecnológica de equipos en los cuales son operativos DIM UCLA y CONSEDE.	3
Emisión de información desactualizada en un momento dado.	3
Envío y recepción de información en formatos no adecuados y fuera de los estándares	3
Dependencia de procedimientos manuales por falta de conexión entre núcleos.	3

1: Bajo 2: Medio 3:Alto

Conclusiones

CONSEDE, conjuntamente con el sistema de carga de maestros DIM UCLA, constituyeron una solución que ciertamente apoyaba la gestión de la Dirección de Mantenimiento de la UCLA. En sus tiempos, los objetivos se lograban sin mayor dificultad, pero a medida que el tiempo fue pasando se incrementaron las debilidades y se hicieron más notorias. Una de sus principales debilidades es ser un sistema independiente de los otros sistemas que soportan la mayoría de las actividades de la UCLA.

El llevar un sistema con las debilidades descritas , hace que la aparición de problemas en el mismo crezca exponencialmente, llegando a límites como no considerar usar el sistema sino que incluyen, modifican, eliminan y consultan directamente desde la base de datos, la cual utiliza ACCESS como herramienta. Con ejemplos como este se puede constatar que no hay garantía de seguridad de datos.

Los sistemas CONSEDE y DIM UCLA no tienen garantías de Auditabilidad, Disponibilidad de Información, Integridad de datos y Confidencialidad de la información; si bien no se manejan claves, clientes, como por ejemplo, un sistema bancario, si se manejan montos de obras, costos de maquinarias y otra información confidencial de la UCLA, esta información está perfectamente accesible para cualquier persona que desee obtenerla (hablando de la seguridad del sistema). Son altamente vulnerables y pueden ser manipularlos convenientemente sin ningún problema.

La búsqueda de una transformación tecnológica y la aplicación de controles de: implementación (referidos al buen uso de los sistemas), de software, de operaciones de computación y de seguridad de datos garantizarán el alcance de objetivos de la mano con herramientas informáticas bien implementadas, cuyo margen de error sea mínimo, que genere información útil para el soporte a la toma de decisiones y que ayude al mantenimiento de los activos de la UCLA, ahorrando a esta casa de

estudios recursos económicos por reemplazo de maquinarias y generando información irrefutable del estado actual y teórico de los mismos, que es el deber ser de todo sistema de gestión de mantenimiento. Así como también un excelente manejo de empleados y su rendimiento.

Recomendaciones

Por toda la problemática que se ha planteado anteriormente, y por la carencia de código fuente que imposibilita cualquier actividad de mejora sobre los sistemas CONSEDE y DIM UCLA, se hacen las siguientes recomendaciones:

1. Realizar una Reingeniería de procesos para de esta forma rescatar las funcionalidades útiles de los sistemas y de esta forma facilitar el levantamiento de información con vías a una nueva construcción de un producto software.
2. Documentar cada paso de la reingeniería de procesos.
3. Migrar los datos de los sistemas a un motor de base de datos que les permita la creación de una base de datos distribuida entre diferentes núcleos del sistema, para así solventar la problemática ocasionada por los módulos independientes.
4. Desarrollar una nueva aplicación software con base a las características anteriormente nombradas y una carta de funciones que integre los nuevos requerimientos como por ejemplo el seguimiento de la gestión del personal de la Dirección de Mantenimiento de la UCLA.
5. Mantener válidas las licencias de antivirus en caso que se contemplen sistemas operativos como Windows, para protección a software malicioso

4.7. Escenario No. 7:

Tipo de Auditoría Informática: Base de Datos

Empresa: Evolution POS C.A.

Programa de Auditoría informática de base de datos aplicado

- Fase Preliminar
  - Planificación de las actividades.
  - Entrevista con el cliente
  - Levantamiento inicial de información
  - Definición de alcance y objetivos de la auditoría.
  - Elaboración de la matriz de análisis de auditoría.
  - Elaboración de los procedimientos de auditoría.
  - Elaboración de entrevistas
  - Elaboración de cuestionarios
  - Elaboración de pruebas de caja negra
- Desarrollo de la Auditoría
  - Entrevista con el personal objeto de Auditoría.
  - Aplicación de cuestionarios y listas de chequeo al personal objeto de auditoría.
  - Observación directa sobre los procesos auditados en la organización.
  - Recopilación de información y documentación relevante al proceso de auditoría.
  - Análisis de la información recopilada.
- Revisión y Elaboración de Informes
  - Elaboración del Informe.
  - Revisión general de los resultados.

Ejecución de la Auditoría

Se aplicó entrevista (anexo F) a todo el personal de la empresa, ya que su tamaño permitió realizar esta labor. Con esta entrevista se busca:

- Determinar la existencia de documentación de objetivos organizacionales, normas, políticas, cargos y funciones.
- Reconocer la importancia del sistema de control de acceso de personal, en la realización de los objetivos organizacionales.
- Conocer la opinión por parte de los directivos y el personal en general, acerca de la plataforma tecnológica usada para la gestión de la base de datos del sistema de control de acceso de personal.
- Conocer la opinión por parte de los directivos acerca del personal designado para gestionar la base de datos del Sistema de Control de Acceso de Personal.

Los resultados de esta entrevista hacen presumir que a pesar de que están documentados los objetivos, cargos, funciones, normas y políticas organizacionales, existe un desconocimiento general de éstas por parte de todo el personal inclusive el personal gerencial. De igual manera se presume que no está definido claramente la figura del administrador de Base de Datos (DBA) lo que ocasiona incertidumbre sobre quien tiene la responsabilidad de gestionar la base de datos del sistema de control de acceso de personal.

Por otro lado, se infiere que la plataforma tecnológica que soporta el sistema de control de acceso de personal es idónea para la ejecución efectiva, eficiente y segura del mismo.

Se aplicó entrevista (Anexo G) al personal de desarrollo, con esta entrevista se busca conocer la opinión acerca de la plataforma tecnológica usada para la gestión de la base de datos del sistema de control de acceso de personal.

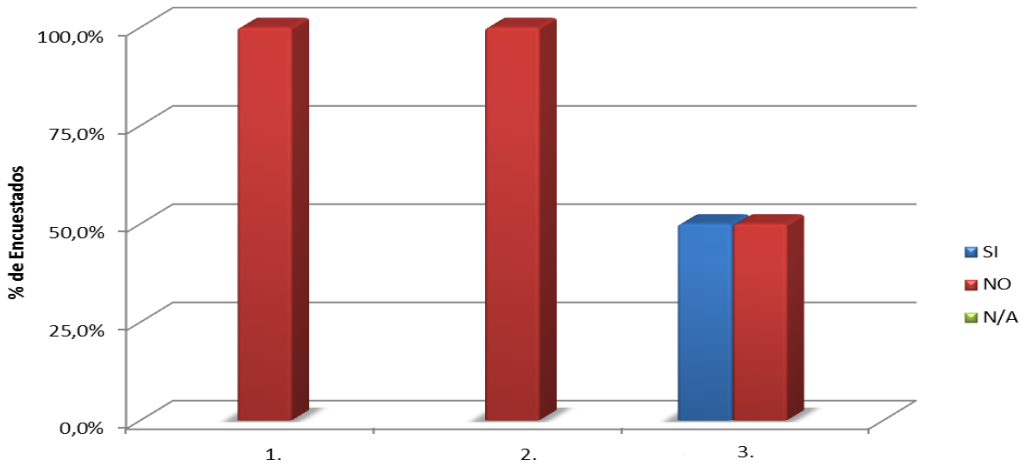
Los resultados de la entrevista apuntan a que la plataforma tecnológica es suficiente para soportar la base de datos del sistema de control de acceso de personal, por otra parte no existe el cargo de administrador de base de datos o DBA pero existen varias personas que realizan las funciones de este rol por lo que se ve afectada de forma negativa el contenido de la base de datos, igualmente no existe formalmente documentación acerca de la base de datos del sistema.

Resultados Cuestionario

Se aplicó cuestionario (Anexo H) al personal de desarrollo. El objetivo de éste instrumento es determinar el grado de integridad y consistencia de datos desde una visión general de la base de datos y de la aplicación.

A continuación se presentan los resultados obtenidos:

Preguntas 1, 2 y 3

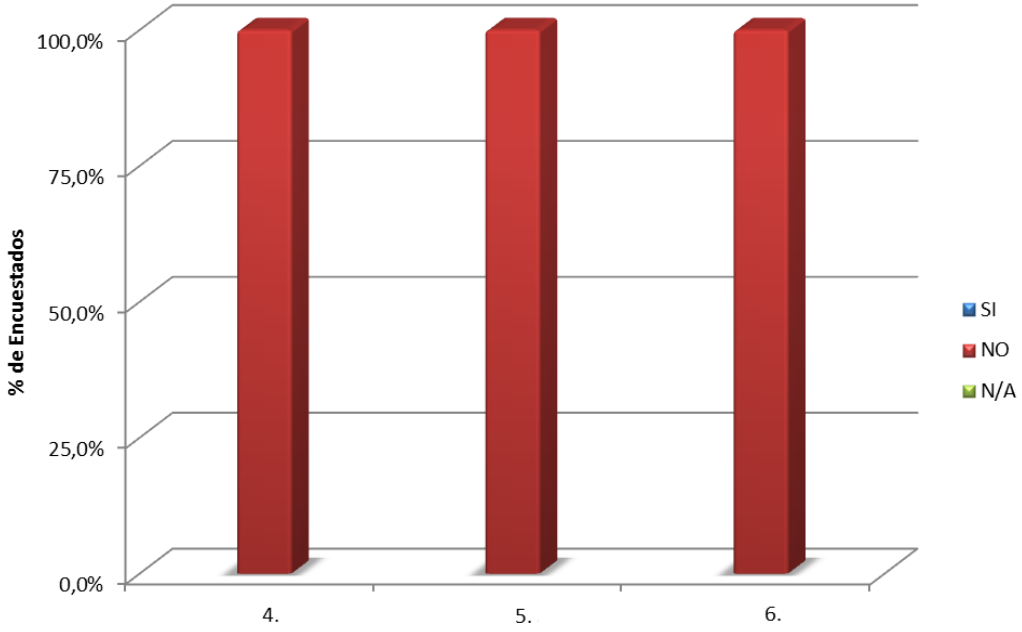


El 100% de los encuestados afirman no usar una metodología para el diseño de bases de datos, de igual manera afirman no utilizar herramientas

automatizadas de soporte para esta labor. Por otro lado, un 50% de los encuestados afirman utilizar alguna de las formas normales estipuladas en el proceso de normalización de bases de datos y otro 50% asegura no utilizar ninguna.

De los resultados obtenidos se presume la inexistencia de una metodología clara para la elaboración del modelo de base de datos para el Sistema de Control de Acceso de Personal, de igual manera, se presume la no utilización de herramientas automatizadas para realizar esta labor.

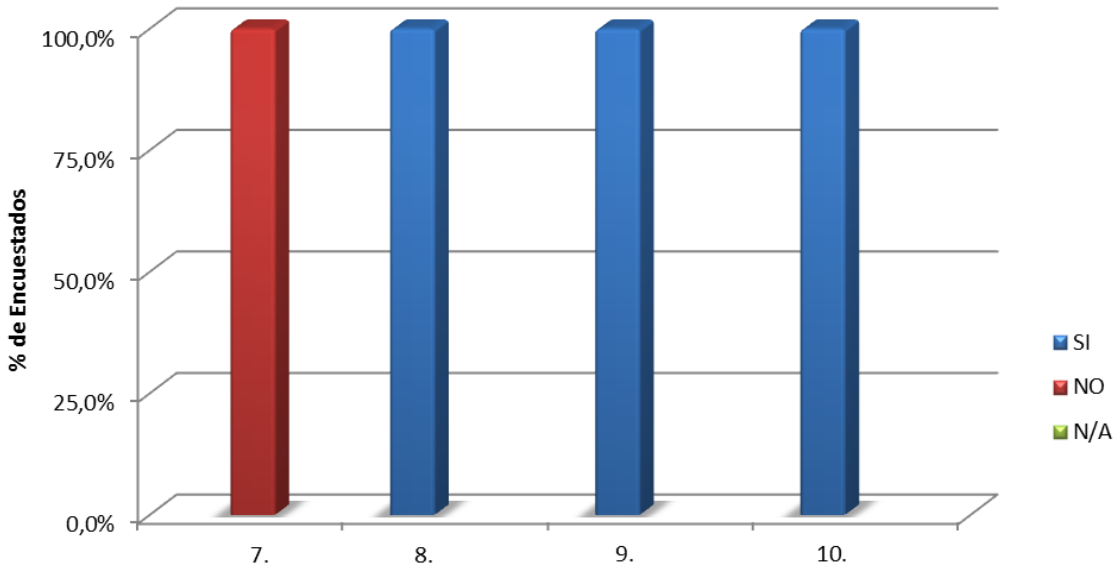
Preguntas 4, 5 y 6



El 100% de los encuestados afirman que no están identificadas y documentadas las tablas maestras, históricas y de transacción para la base de datos del Sistema de Control de Acceso de Personal.

De los resultados obtenidos se infiere la inexistencia de documentación referente a la clasificación de los tipos de tablas para la base de datos del Sistema de Control de Acceso de Personal.

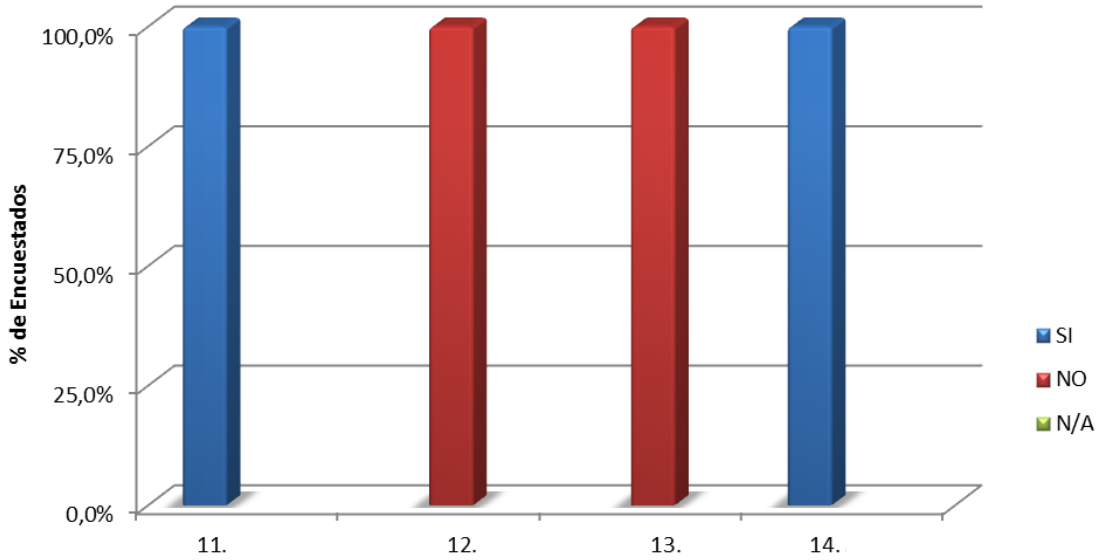
Preguntas 7, 8, 9 y 10



El 100% de los encuestados afirman que no están definidas las cardinalidades entre las tablas de la base de datos del Sistema de Control de Acceso de Personal, Sin embargo el 100% de ellos también afirma que se aplica la eliminación lógica de registros, validación en la eliminación de registros en tablas que afecten a otras tablas y la existencia de consistencia entre la información ingresada al sistema y la información almacenada en la base de datos.

De los resultados obtenidos se presume que a pesar de no estar documentadas la cardinalidad o relaciones entre tablas de la base de datos para el Sistema de Control de acceso de Personal, existe cierto grado de integridad y consistencia en la información debido a validaciones lógicas en la eliminación de datos.

Preguntas 11, 12, 13 y 14



El 100% de los encuestados afirman la existencia de validación a nivel de formularios para el ingreso de información a la base de datos del Sistema de Control de Acceso de Personal, Por otro lado, también afirman no utilizar transacciones ni rollback pero si el commit en operaciones de almacenamiento en la base de datos.

De los resultados obtenidos se infiere que a pesar de la validación de los datos a nivel de aplicación en los formularios, existe una gran posibilidad de que la información se corrompa, el no manejar transacciones en operaciones de almacenamiento ocasiona inconsistencias en los datos al presentarse cualquier fallo durante la realización de este proceso.

Se aplicó cuestionario (Anexo I) a todo el personal gerente, administrativo y operacional ya que interactúan de forma directa con el sistema de control de acceso de personal.

A continuación se presenta los resultados obtenidos para cada pregunta del cuestionario.

ÍTEM	SI	NO	N/A
1	50%	25%	25%
2	50%	37,5%	12,5%
3	87,5%	12,5%	
4	50%	50%	
5	50%	37,5%	12,5%
6	50%	37,5%	12,5%
7		62,5%	37,5%
8	37,5%	25%	37,5%

Ítem 1: Se infiere que la información brindada por el Sistema de Control de Acceso de Personal es la necesaria para la realización de las labores de cada uno de los usuarios del sistema. Sin embargo existe un pequeño porcentaje que en su mayoría son usuarios de la parte gerencial de la organización y consideran aún falta información para la realización óptima de sus labores.

Ítem 2: Se presume que no se debe descartar la incorporación de mayor información a los usuarios, en especial los usuarios administrativos ya que consideran que existe información que aún no maneja el sistema y que puede ser útil para el desempeño de sus funciones.

Í**tem 3:** Se infiere una gran confianza en la información que brinda el Sistema de Control de Acceso de Personal, por lo que se presume que los datos contenidos en la base de datos son íntegros.

Ítem 4: Se presume que existe una alta ocurrencia de problemas de desempeño, las cuales están por encima de los niveles aceptables.

Ítem 5: Los resultados hacen presumir que se tiene un buen manejo de la concurrencia de usuarios al acceder a los datos contenidos en la base de datos del Sistema de Control de Acceso de Personal.

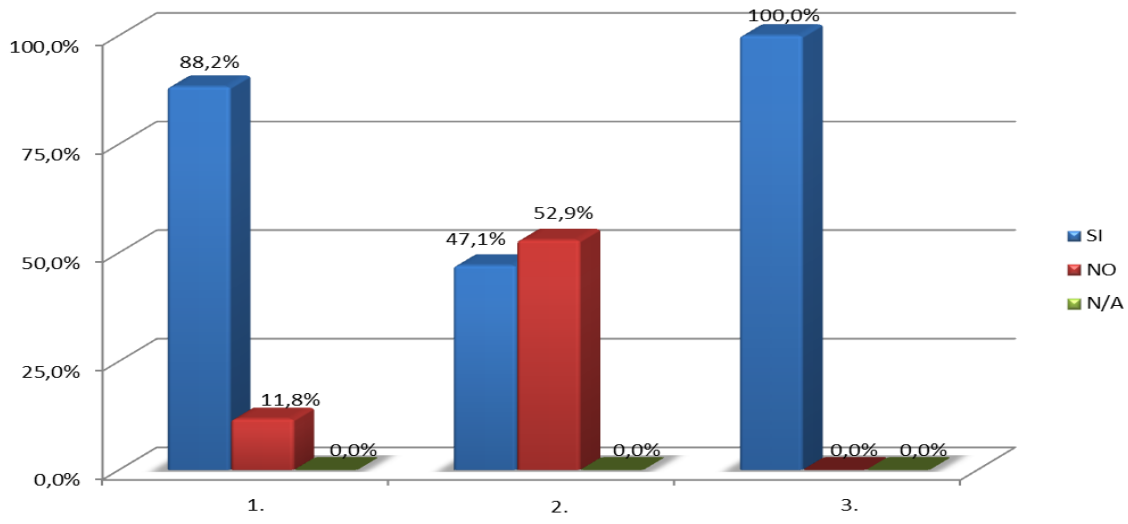
Ítem 6: Se presume a partir de los resultados obtenidos que existen problemas de desempeño durante la ejecución del sistema de Control de Acceso de Personal

Ítem 7: De la información recopilada se infiere que las configuraciones de seguridad y privilegios de usuario a nivel de la aplicación están bien implementados, por lo que no existe problema para los usuarios en acceder a la información necesaria para la realización de sus funciones.

Ítem 8: Los resultados obtenidos hacen presumir que la mayoría de los usuarios pueden acceder de manera oportuna a los reportes impresos con la información que necesiten, sin embargo existe un porcentaje considerable que afirma no poder acceder a dichos reportes.

Se aplicó lista de chequeo (anexo J) a cada una de las tablas de la base de datos (17 en total) del Sistema de control de Acceso de Personal, para de esta manera, determinar la calidad de los datos contenidos en ella.

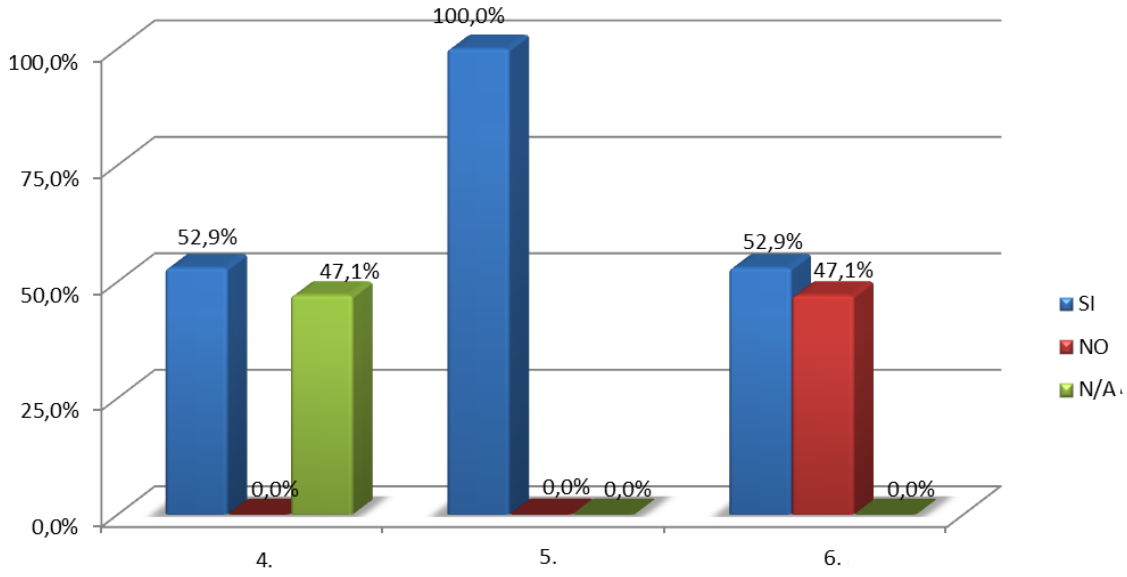
Características 1, 2 y 3



- El 88,2% de las tablas chequeadas posee atomicidad en todos sus campos, un 11,8% no la posee en al menos un campo y el 0% no aplica esta característica.
- El 47,1% de las tablas tiene clave primaria, un 52,9% no la tiene y el 0% no aplica esta característica.
- El 100% no posee grupos de datos repetidos.

A partir de los resultados obtenidos se presume que existe un buen diseño de la base de datos basando en reglas de normalización, sin embargo la mayoría de las tablas no posee claves primarias por lo que se podría perjudicar la integridad y unicidad de los campos en la base datos del Sistema de Control de Acceso.

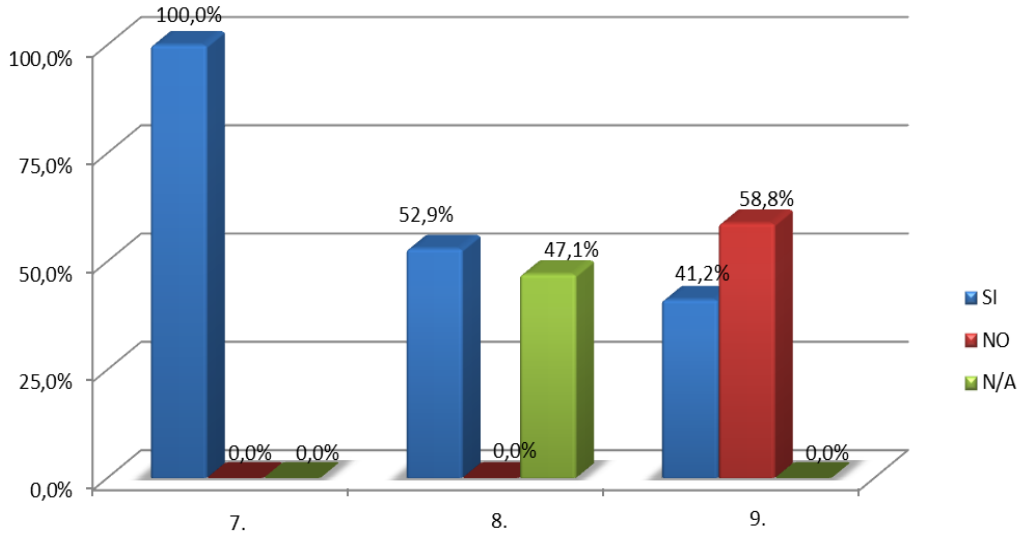
Características 4, 5 y 6



- El 100% tiene sus campos no claves independientes mutuamente.
- El 52,9% de las tablas usan claves foráneas, un 47,1% no la usan y el 0% no aplica esta característica.

Se presume en base a los resultados obtenidos la existencia de un buen diseño de base de datos y uso de reglas de normalización, a pesar de que un gran porcentaje de las tablas no usa claves foráneas, cabe destacar que en su mayoría son tablas maestras por lo que el uso de claves foráneas puede ser opcional no implicando esto un mal diseño de base de datos.

Características 7, 8 y 9



- El 100% de las tablas chequeadas almacena los valores para una misma columna en un mismo formato
- El 52,9% de las tablas poseen consistencia entre los nombres, tipo de datos y longitud de campos relacionados con otros campos en otras tablas, el 0% no la posee y un 47,1% no aplica esta característica.
- El 41,2% de las tablas poseen índices para sus principales campos de búsqueda, el 58,8% no los poseen y el 0% no aplica esta característica.

De los resultados obtenidos se infiere una gran consistencia en los valores almacenados en la base de datos, sin embargo la mayoría de las

tablas no posee índices lo que supondría problemas de desempeño al momento de realizar consultas sobre la información contenida en la base de datos.

Resultados Pruebas de Software (Caja Negra)

El resultado de las pruebas fue satisfactorio, se demostró que para el formulario de gestión de empleados, se valida la entrada de datos y se registra el usuario en la base de datos.

- **Dimensión:** Seguridad Lógica.

Resultados Pruebas de Software (Caja Negra)

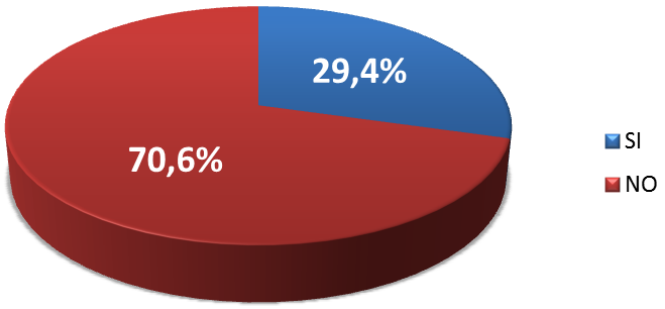
El resultado de las pruebas fue satisfactorio, se demostró que el manejo de privilegios y control de acceso a nivel de la aplicación es efectivo.

Se recurrió a la observación directa, pruebas de software y documentación suministrada por la organización. El objetivo es identificar las políticas, normas de seguridad, gestión de respaldo y recuperación existentes en la organización para la gestión de la base de datos del Sistema de Control de Acceso de Personal.

Característica a Chequear	SI	NO
1. Control de acceso a nivel de base de datos.	**X**	
2. Documentación de los perfiles de seguridad por los cuales se tendrá acceso a la base de datos.		**X**
3. Plantillas de perfiles de seguridad (scripts) definidas para la creación de usuarios en la base de datos.		**X**
4. Control de acceso a nivel de la aplicación.	**X**	
5. Abstracción de la información mediante vistas para el usuario.		**X**
6. Validación y Manejo de errores en la entrada de datos.	**X**	
7. Claves de usuarios encriptadas.		**X**
8. Metodología para la recuperación y cambio de contraseñas a nivel de aplicación.		**X**

9. Protección de la información sensible para los usuarios y la organización.		**X**
10. Reporte de acceso al sistema a nivel de la aplicación.	**X**	
11. Rastreo de responsable y fecha de modificación de registros para tablas maestras.		**X**
12. Respaldos periódicos de la base de datos.	**X**	
13. Planes de acción en caso de violaciones a las medidas de seguridad de la base de datos.		**X**
14. Definición y documentación de los períodos de almacenamiento de datos de respaldo.		**X**
15. Existencia de personal encargado de gestionar los respaldos de base de datos		**X**
16. Plan de gestión para el control de los archivos de auditoría LOG.		**X**
17. Existencia de personal encargado de gestionar el control de los archivos de auditoría LOG.		**X**

Gráfica de resultados



El gráfico anterior describe el grado de cumplimiento de la lista de características, con lo que se obtienen los siguientes resultados:

Solo el 29,4% de las características evaluadas se cumplen y un 70,6% no.

Con la información obtenida se infiere que a nivel de la aplicación se maneja de manera básica las validaciones respectivas para la gestión de la seguridad, como lo son: Manejo de errores en entrada de datos, control de acceso y reportes de acceso al sistema. Sin embargo, a nivel del sistema de

gestión de base de datos se detectó la inexistencia de documentación de perfiles de seguridad y planes de acción en caso de violaciones de seguridad, de igual forma, no existe un personal encargado de gestionar los archivos de auditoría LOG y los respaldo de bases de datos, por lo que existe a nivel general un gestión deficiente del manejo de la seguridad lógica de la base de datos.

Matriz de Riesgo

Descripción del riesgo	Impacto	Probabilidad
Conflicto entre las funciones del administrador de base de datos (DBA).	2	3
Dependencia crítica sobre el personal designado como DBA.	3	2
Ingreso de información incoherente por parte de los usuarios de la aplicación.	3	1
Accesos no autorizados por personal interno o externo a la organización.	3	2
Fallas en la red de datos de la organización.	3	1
Cambios repentinos en el personal encargado de administrar la base de datos.	3	1
Manejo inadecuado de las claves personales por parte de los usuarios.	3	3
Nuevos requisitos de información por parte de la organización	3	1
Normas y políticas gubernamentales que afecten la utilización del sistema o la base de datos directamente.	3	1
Inexistencia de documentación de los planes de acción en caso de violaciones de acceso	2	3
Desconocimiento por parte del personal acerca de las funciones inherentes a sus cargos	3	2

Impacto: 1: Bajo, 2: Medio, 3: Alto

Probabilidad: 1: Baja, 2: Media, 3: Alta

Hallazgos Detectados

1. Existencia de documentación referente a los objetivos generales, objetivos específicos, cargos, funciones, organigrama y normas organizacionales, sin embargo se presume que no existe documentación acerca de las políticas organizacionales.

2. Se presume que la mayoría del personal gerente y operativo desconoce los objetivos de la organización.
3. Con la información recolectada se infiere que la mayoría del personal desconoce sus funciones dentro de la organización, por lo que tienden a mezclarse con la de otros cargos.
4. Se presume que a pesar de que el personal conoce las normas organizacionales, éstas no se aplican en su totalidad.
5. De la información recopilada se especula que el organigrama y demás información referente a los objetivos organizacionales no está accesible ni visible fácilmente por el personal de la empresa.
6. Se presume que dentro del organigrama de la empresa no existe un cargo definido para la gestión de base de datos (DBA).
7. Se especula que el personal del departamento de desarrollo tiene acceso a la información contenida en la base de datos del Sistema de Control de Acceso de Personal, la cual los afecta directamente en el pago de las horas laboradas en el mes, lo que implica un conflicto de intereses.
8. Se infiere que la plataforma tecnológica (Sistemas operativos, enrutadores, switches, cableado estructurado, lenguajes de programación, sistemas de gestión de base de datos) es óptima para el desempeño efectivo, eficiente y seguro del sistema de control de acceso de personal.
9. Se presume que no existe ninguna metodología a seguir para el diseño de bases de datos.
10. De la información recopilada se desprende la aplicación de reglas de normalización para el diseño de la base de datos del Sistema de Control de Acceso de Personal, sin embargo, se descuidan buenas prácticas para el desempeño de la base de datos como lo es la creación de índices en las tablas para campos de búsqueda.

11. De la información obtenida de las entrevistas y cuestionarios realizados a los usuarios se deduce un alto de grado de confiabilidad, consistencia, completitud e integridad de la información contenida en la base de datos, sin embargo, se presume la existencia de un margen elevado de problemas de disponibilidad de la información.
12. Se presume la inexistencia de documentación para planes de respaldo y recuperación de bases de datos, así como para la gestión de archivos de auditoría LOG y planes de acción en caso de violaciones a las medidas de seguridad de la base de datos.

Conclusiones

El proceso de gestión de base de datos constituye una de las ramas más amplias de la informática, desde su diseño, pasando por la elaboración, implementación y seguimiento, son muchos los aspectos y controles que se deben evaluar.

Durante el proceso de auditoría informática de base de datos de la empresa Evolution POS, se detectaron una gran cantidad de deficiencias a nivel organizacional, documental y de planificación, lo que hace suponer que no se estipula ninguna metodología clara para la realización de las funciones de administración y control de la base de datos, esto trae como consecuencia que el conocimiento y experiencia de las actividades relacionadas con el manejo de la base de datos, pertenezcan solo al personal y no a la organización, lo que supone un riesgo, ya que se depende de una persona para la realización de actividades críticas sobre la base de datos.

Por otra parte, a pesar de no tener un modelo de diseño de bases de datos a seguir, cabe destacar que existe un alto grado de consistencia, integridad y confiabilidad en los datos almacenados en la base de datos del sistema de control de acceso de personal. Sin embargo se descuidan

características como el desempeño y la disponibilidad de la información, ya que la mayoría del personal asegura haber presentado problemas de este tipo.

En cuanto a la seguridad, se infiere la existencia de un alto grado de medidas de control a nivel de la aplicación, no obstante existen ciertos vacíos en la seguridad a nivel del Sistema de Gestión de Bases de Datos, además de que se presume la inexistencia de documentación alguna referente a este tópico.

Recomendaciones

La definición de los objetivos dentro de una empresa, constituye uno de los principales procesos organizacionales, ya que allí se determinan las metas que se deben lograr y como se deben lograr. Es por ello que el desconocimiento de los objetivos por parte del personal, implica un riesgo funcional donde los esfuerzos podrían no ir dirigidos hacia un fin común.

En base a lo anterior se proponen las siguientes recomendaciones:

1. Se recomienda definir y documentar las políticas organizacionales, además de velar por la aplicación de estas.
2. Se sugiere propulsar el conocimiento e internalización de los objetivos de la organización por parte del personal, a través de reuniones y minutas, en especial para el personal estratégico ya que son ellos los encargados de tomar las decisiones que afectan el rumbo de la empresa.
3. Se recomienda definir claramente los cargos y funciones dentro de la organización, y garantizar el conocimiento de estas por parte del personal.
4. Se sugiere colocar de manera accesible en un lugar visible fácilmente el organigrama, misión, visión y objetivos generales de la organización, para de esta manera fomentar la identificación del

personal con la organización y enfocar los esfuerzos hacia un objetivo común.

En el mismo sentido, cabe destacar que los DBA son personas de vital importancia en el manejo y administración de una base de datos, ya que se encargan de una serie de tareas como lo es la creación y recuperación de respaldos, verificación de integridad de los datos, definición e implantación de controles de acceso a los datos, aseguramiento de condiciones óptimas de desempeño y confiabilidad de la información, colaboración con desarrolladores en el uso eficiente de la base de datos, entre otras. Por lo que se recomienda lo siguiente:

1. Se recomienda la designación de un personal que se encargue de realizar la gestión de la base de datos del sistema de control de acceso de personal (DBA), el cual apropiadamente estaría en un alto nivel dentro del organigrama de la empresa, esto con la finalidad de evitar conflicto de intereses entre sus funciones y lograr la segregación de estas.
2. Se sugiere la implantación de una metodología clara para la elaboración y diseño de bases de datos.
3. Se recomienda la incorporación de una mayor planificación y documentación sobre los procesos de seguridad y recuperación que se deben aplicar a la gestión de base de datos del Sistema de Control de Acceso de Personal.

4.8. Escenario No. 8:

Tipo de Auditoría Informática: Mantenimiento SISTEMA SAT-MANAGER

Empresa: CompuAmigo C.A.

Programa de Auditoría informática de Mantenimiento aplicado

- Fase Preliminar
  - Entrevista inicial al cliente.
  - Levantamiento inicial de información.
  - Elaboración de Programa General.
  - Elaboración de Programas de Procedimientos.
  - Elaboración de Matriz de Análisis.
  - Elaboración de los procedimientos de auditoría.
  - Elaboración de entrevistas
  - Elaboración de cuestionarios
- Desarrollo de la Auditoría
  - Entrevista con el gerente.
  - Aplicación de cuestionario.
  - Observaciones directas de las instalaciones.
  - Discusión de la metodología empleada para el procesamiento de la información obtenida.
  - Procesamiento y/o tabulación de la información obtenida.
- Revisión y Pre-informe
  - Revisión de la Información obtenida.
  - Elaboración del Informe

Matriz de Riesgos

MR

Descripción del Riesgo	Impacto	Probabilidad
Ausencia de Fallas	3	3
Datos de prueba muy generales	1	2
Insuficiencia de pruebas	1	1
Tiempo de prueba muy corto	2	1
Prueba con datos que nunca han presentado fallas	3	3
Poco volumen de información almacenada	3	2

Impacto: 1: Bajo, 2: Medio, 3: Alto

Probabilidad: 1: Baja, 2: Media, 3: Alta

Fase de Ejecución

Analisis e Interpretación de los resultados obtenidos:

Observación:

CUESTIONARIO DE OBSERVACIÓN				
DIMENSION	ITEM	CONSULTA	RESPUESTA	
			SI	NO
Seguridad	1	Existen perfiles de usuario para el uso del sistema		X
	2	Permite realizar un respaldo de la información	X	
	3	Permite llevar un registro las transacciones claves		X
Capacidad de Cambio	4	Permite llevar un registro de los cambios		X
	5	Es fácil de incluir o modificar los parámetros		X
	6	Esta diseñado para que pueda cambiar en el tiempo	X	
Controles Automáticos	7	El sistema operativo posee claves de uso		X
	8	Los equipos poseen capta huellas		X
	9	El sistema operativo permite llevar un registro de transacciones		X
Entradas	10	Los datos de entrada poseen redundancia		X
Salidas	11	Es aceptable el promedio en el tiempo de respuesta	X	
Análisis de la Información Obtenida	12	Se está ejecutando en forma correcta el proceso de información	X	
	13	Cumple el sistema con lo que se esperaba	X	
	14	En General, se puede mejorar el sistema	X	

CUESTIONARIO APLICADO AL USUARIO:

CU

CUESTIONARIO DE USUARIO				
Nombre:		**Cargo:** TÉCNICO DE SOPORTE A USUARIO		
DIMENSION	**ITEM**	**CONSULTA**	**RESPUESTA**	
			SI	**NO**
Desempeño	1	Durante el mes, permanece mucho tiempo inactivo por fallas		X
	2	Es suficiente el tiempo cuando funciona bien	X	
	3	Es poco el tiempo entre una falla y la siguiente		X
Contrato de Mantenimiento	4	Cuando falla, se le notifica al fabricante	X	
Entradas	5	Es necesario incluir otros datos que complementen la información		X
	6	Se solicitan datos que luego no se utilizan		X
Salidas	7	Presenta un alto porcentaje de satisfacción de los resultados	X	
	8	Presenta un alto porcentaje de fallas		X

ENTREVISTA REALIZADA AL GERENTE:

CUESTIONARIO DE ENTREVISTA				
Nombre:		**Cargo:** DIRECTOR GERENTE		
DIMENSION	**ITEM**	**CONSULTA**	**RESPUESTA**	
			SI	**NO**
Uso de los Recursos	1	Se usa el sistema durante toda la jornada laboral	X	
	2	El usuario fue capacitado por el fabricante antes de utilizarlo		X
	3	Existen reglas o políticas definidas para el uso	X	
Contrato de Mantenimiento	4	Existe un contrato de mantenimiento		X
	5	Existe algún plan de mantenimiento preprogramado		X
Procesos	6	En general, se considera aceptable la ejecución de los procesos	X	
	7	Los procesos pueden ser mas sencillos		X
	8	Pueden interactuar con otros proceso	X	

Metodología de control interno

Para hallar el porcentaje de cumplimiento de cada una de las dimensiones, tomamos como referencia la formula matemática:

- Para hallar el SI

  25 ----------►100%

  18 ----------►X

  X = 72

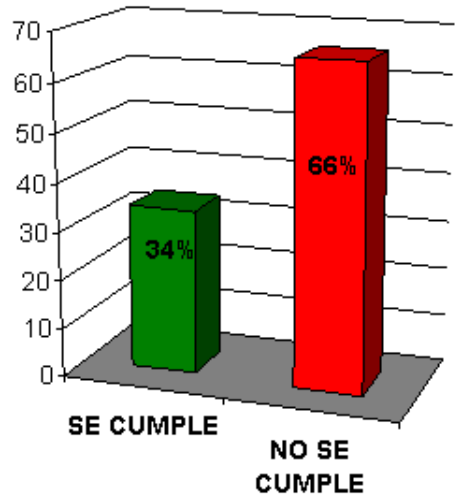
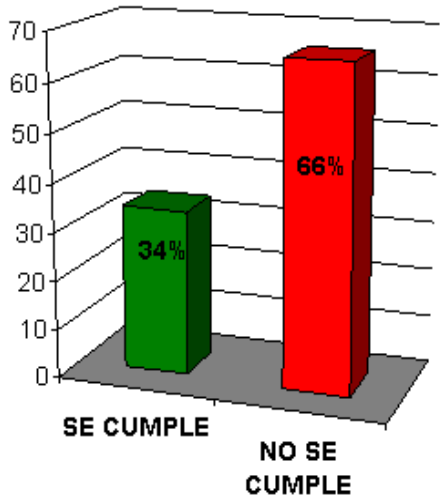
- Para hallar el NO

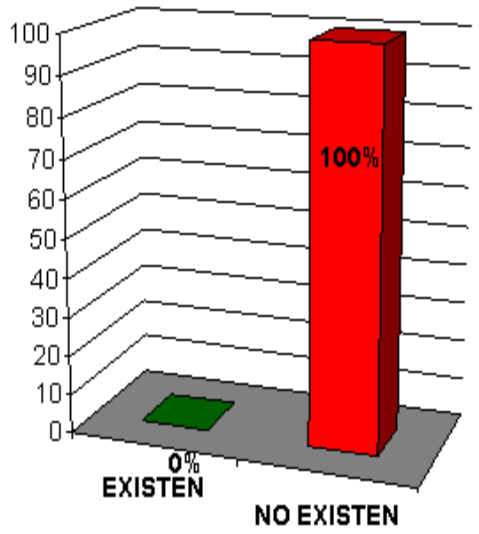
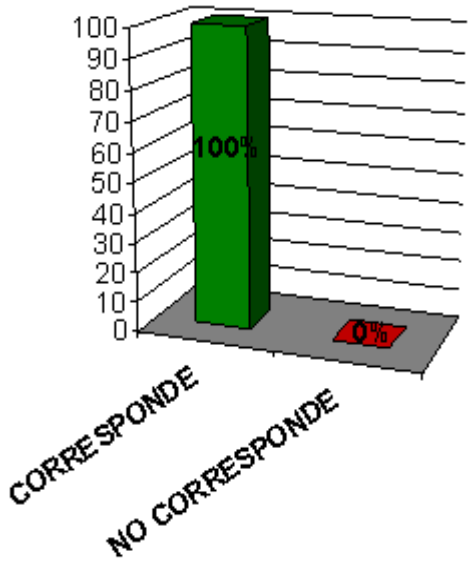
  25 ----------► 100%

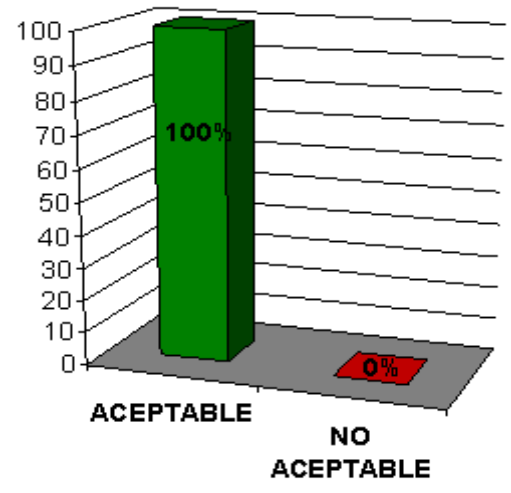
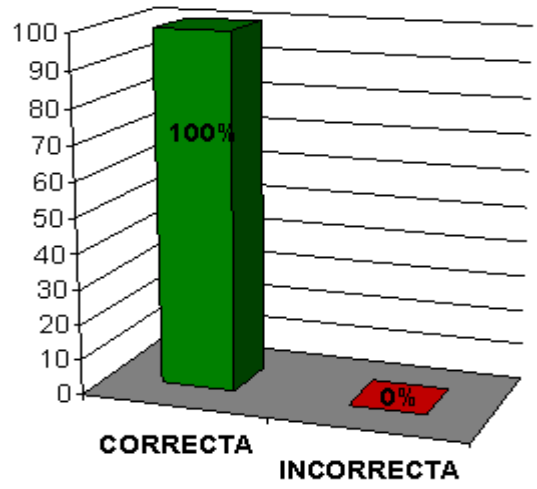
  7 ----------► X

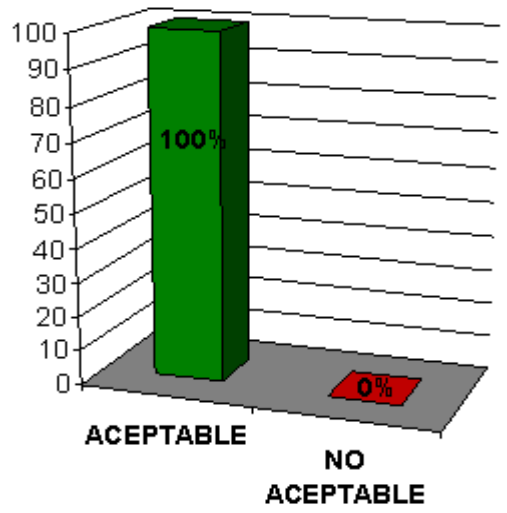
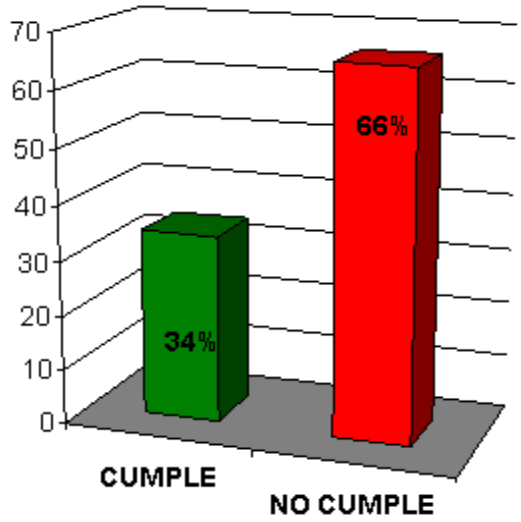
  X = 28

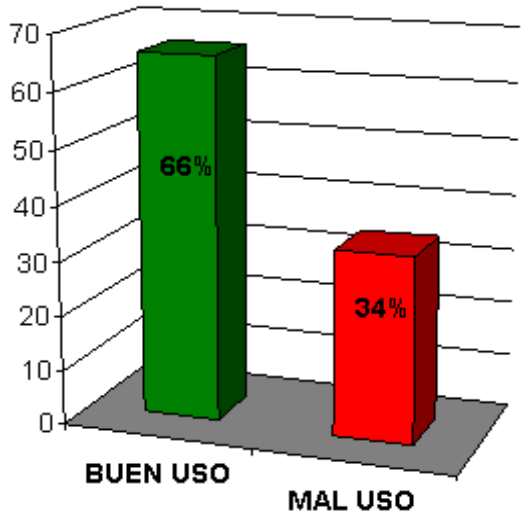
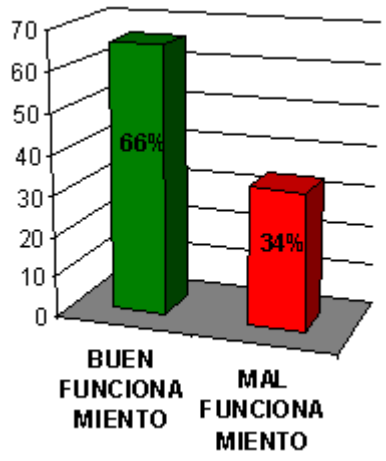
ANÁLISIS GRÁFICO DE LOS RESULTADOS:

Indicadores de Seguridad del Sistema:	Indicadores de Capacidad de Cambio del Sistema:
	

Indicadores de la Existencia los Controles Automáticos Establecidos por la Gerencia para el Uso de los Sistemas:	Indicadores de la Correspondencia de los Datos de Entrada Solicitados para Alimentar el Sistema:
	

Indicadores de la Aceptabilidad de los Datos de Salida Generados por el Sistema Luego de Realizar los Procesos:	Indicadores del Análisis de la información Obtenida al hacer uso del Sistema:
	

Indicadores del Desempeño General del Sistema:	Indicadores del Cumplimiento del Contrato de Mantenimiento del Sistema:
	

Indicadores del Uso de los Recursos:	Indicadores del Funcionamiento de los Procesos:
	

Hallazgos de Auditoría

1. Pérdida de controles
2. Pérdida de una fuente de aprendizaje, porque una actividad interna pasa a ser externa.
3. Dependencias del Proveedor.
4. Uso de metodologías para nuevos desarrollos, pero ausencia de ellas para el mantenimiento.
5. Dificultad progresiva de modificación del sistema.

Conclusiones

1. Como resultado de la Auditoria del Mantenimiento realizada a la Empresa CompuAmigo C. A., se ha cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
2. El área de Informática trabaja en consonancia con lo que se ha estipulado en sus funciones.

Recomendaciones

1. Modificación de un producto software, o de ciertos componentes, usando para el análisis del sistema existente técnicas de Ingeniería Inversa y, para la etapa de reconstrucción, herramientas de Ingeniería Directa, de tal manera que se oriente este cambio hacia mayores niveles de facilidad en cuanto a mantenimiento, reutilización, comprensión o evolución y seguridad.
2. Categorizar los tipos de mantenimiento del software y para cada tipo planificar las actividades y tareas a realizar.
3. Establecer un acuerdo o contrato de mantenimiento entre el mantenedor y el cliente y las obligaciones de cada uno estos.

4. Elaborar un plan de mantenimiento que incluya el alcance del mantenimiento, quién lo realizará, una estimación de los costes y un análisis de los recursos necesarios.

4.9. Escenario No. 9:

Tipo de Auditoría Informática: Desarrollo. SISTEMA DE PRODUCCIÓN

Empresa: Azucarera Río Turbio C.A.

Programa de Auditoría informática de Desarrollo aplicado

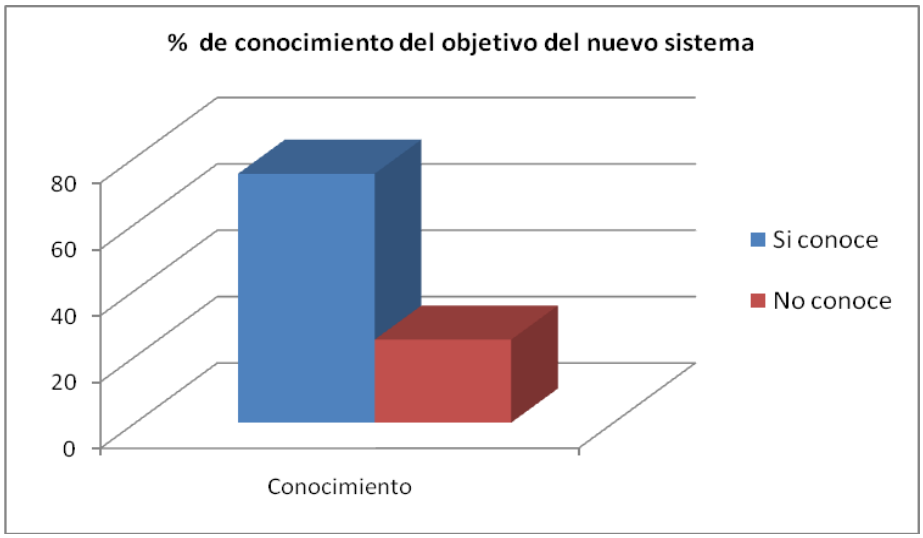
- Fase Preliminar
  - Solicitud de Manuales y Documentación.
  - Levantamiento de información: estructura organizativa, visión y misión, recursos humanos, tecnológicos y financieros del área de sistemas.
  - Elaboración de los cuestionarios
- Desarrollo de la Auditoría
  - Aplicación de cuestionarios al personal de desarrollo.
  - Entrevistas a líderes de áreas y usuarios claves de Producción.
  - Evaluación de los controles internos en cada fase de desarrollo.
- Revisión y Elaboración del Informe
  - Revisión de los papeles de trabajo.
  - Determinación del diagnóstico e incidencias.
  - Elaboración del Informe

Ejecución de la Auditoría

La mayoría de las gerencias que conforman la empresa tienen sus procesos sistematizados; sólo la Gerencia de Producción continúa monitoreando sus procesos de manera manual, con ayuda de complejas plantillas elaboradas en Excel y elaborando sus estadísticas e indicadores de gestión a través de la recopilación de datos y cifras que proporcionan cada departamento de forma aislada y en diferentes formatos.

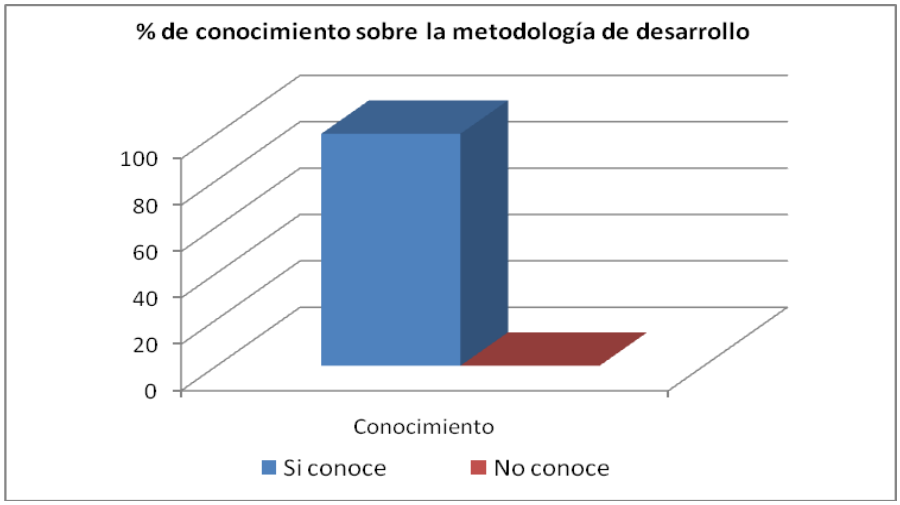
Es por ello que la Gerencia General aprobó un proyecto para el desarrollo de un sistema para Producción, a cargo de la Gerencia de Sistemas, con la finalidad de llevar un control automatizado de sus operaciones y que permita conocer los resultados de cada departamento en cualquier momento, obtener indicadores de gestión y facilitar la toma de decisiones a los niveles gerenciales.

Se aplicó la entrevista al Gerente de Producción de la empresa y a cada uno de los Jefes de las áreas a sistematizar. Del análisis de los resultados de dichas entrevistas se pudo conocer, entre otros, el porcentaje de supervisores de la Gerencia de Producción que posee conocimiento sobre el objetivo del nuevo sistema. A continuación se describe el resultado.

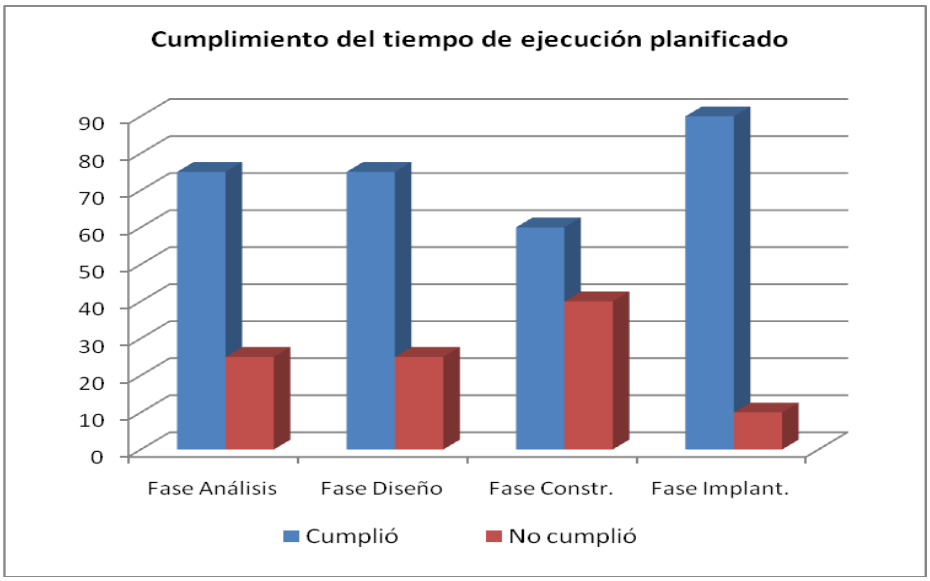


El gráfico indica que de un total de 8 entrevistados, el 75% posee conocimiento sobre el objetivo del nuevo sistema a desarrollar, mientras que el 25% no conoce el objetivo; por lo que se presume que no hubo total divulgación del proyecto hacia todas las áreas involucradas.

De la aplicación del cuestionario al personal del Área de Ingeniería de Software se obtuvo los siguientes resultados:



El gráfico demuestra que el 100% del personal del Área de Ingeniería de Software posee conocimientos sobre la metodología de desarrollo usada.



El gráfico indica el porcentaje del cumplimiento del tiempo planificado en la ejecución de cada fase:

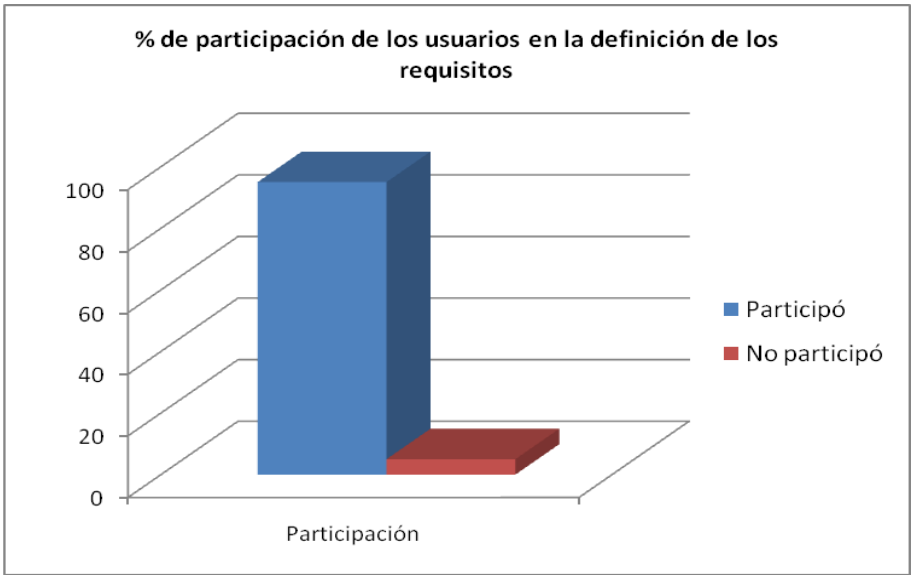
- Fase de análisis, se cumplió en un 75%.
- Fase de diseño, se cumplió en un 75%.
- Fase de construcción, se cumplió en un 60%.
- Fase de implantación y pruebas, se cumplió en un 90%.

Estos resultados parecen indicar que no existe una gestión del proyecto de desarrollo en el seguimiento de los tiempos establecidos para cada fase.

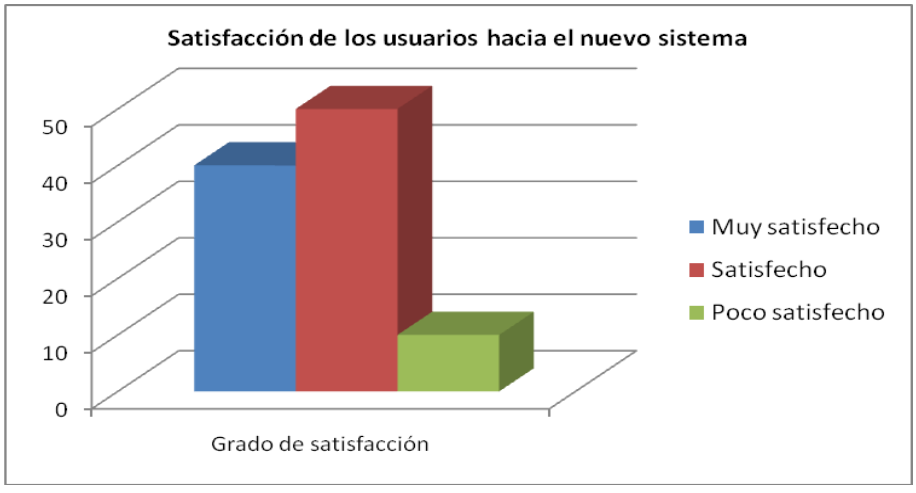
Se realizó la entrevista a cada uno de los usuarios del nuevo sistema, obteniendo resultados muy relevantes, tales como: participación de los usuarios en la definición de los

requisitos, grado de satisfacción hacia el nuevo sistema, complejidad del nuevo sistema, entre otros.

En los gráficos mostrados a continuación se pueden observar algunos de estos resultados.



El gráfico nos indica que un 95% de los usuarios del nuevo sistema participaron en la definición de los requisitos de su área.



El gráfico nos ayuda a identificar el grado de satisfacción de los usuarios hacia el nuevo sistema: un 40% de los usuarios están muy satisfechos, el 50% están satisfechos, mientras el 10% manifestó sentirse poco satisfecho; este último resultado corresponde, probablemente, a los usuarios que manifestaron no haber participado en la definición de los requisitos.

Matriz de Riesgos

Descripción del Riesgo	Impacto	Probabilidad
El proyecto no tiene suficiente apoyo de la gerencia	3	1
Se agregan nuevas especificaciones al proyecto	3	2
La planificación está basada en recursos no disponibles	2	1
No se cuenta con personal, herramientas, materiales y/o equipos de trabajo a tiempo	3	1
No se cuenta con personal con la experiencia técnica necesaria	3	1
Las pruebas del producto requiere más tiempo que el esperado	2	1
Los usuarios finales no se involucran en el desarrollo del proyecto	3	2
El producto no satisface al usuario final	3	2

Impacto: 1: Bajo, 2: Medio, 3: Alto

Probabilidad: 1: Baja, 2: Media, 3: Alta

Hallazgos de auditoría

1. No hubo difusión del objetivo del nuevo sistema hacia todas las Jefaturas de áreas involucradas en el proyecto.

2. Ausencia de un seguimiento del plan de proyecto de desarrollo.
3. Incumplimiento en los tiempos de entrega de los productos.
4. No existe documentación de los cambios realizados en cada fase de desarrollo del nuevo sistema.

Conclusiones

1. Como resultado de la auditoría informática se puede mencionar que se cumplió en su totalidad la evaluación de los objetivos planteados en el programa de auditoría.
2. Se intuye que el área de Ingeniería de Software presenta deficiencias en la administración de proyectos en lo que se refiere al seguimiento que garantice el cumplimiento de los tiempos de entregas establecidos.

Recomendaciones

1. Planificar campañas de comunicación y difusión a las áreas de la organización involucradas en cualquier proyecto de desarrollo o mantenimiento de software.
2. Asignar un responsable del equipo para cada proyecto, quien se encargue de realizar un seguimiento estricto a los tiempos programados para cada fase, a fin de que se tomen con anticipación medidas que aminoren los retrasos en la entrega de los productos.
3. Diseñar y hacer uso de formularios en los que se documenten todos los cambios realizados en cada fase del proyecto, con su debida justificación.

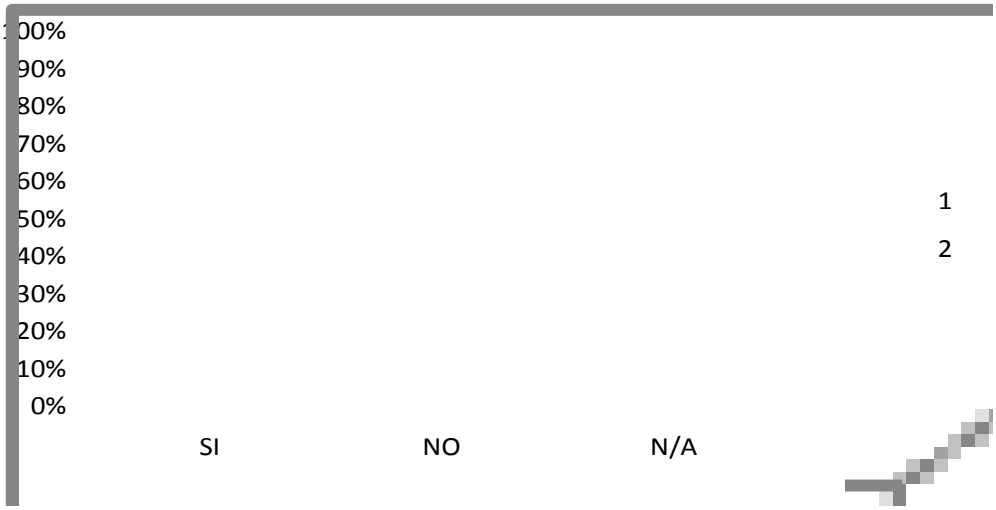
A los efectos de apoyar la propuesta de una metodología de AuditorÍa para la revisión de sistemas de información, se presenta a continuación los resultados correspondientes a la aplicación del

cuestionario (Anexo K) a Profesionales Expertos en el área de Informática :

Análisis de los resultados de la aplicación de cuestionarios a los profesionales del área en informática

Ítem 1 y 2

Dimensión: Evaluación de los Sistemas de Información y Conocimiento de la metodología de Auditoría informática.



Fuente: Cuestionario aplicado a expertos.

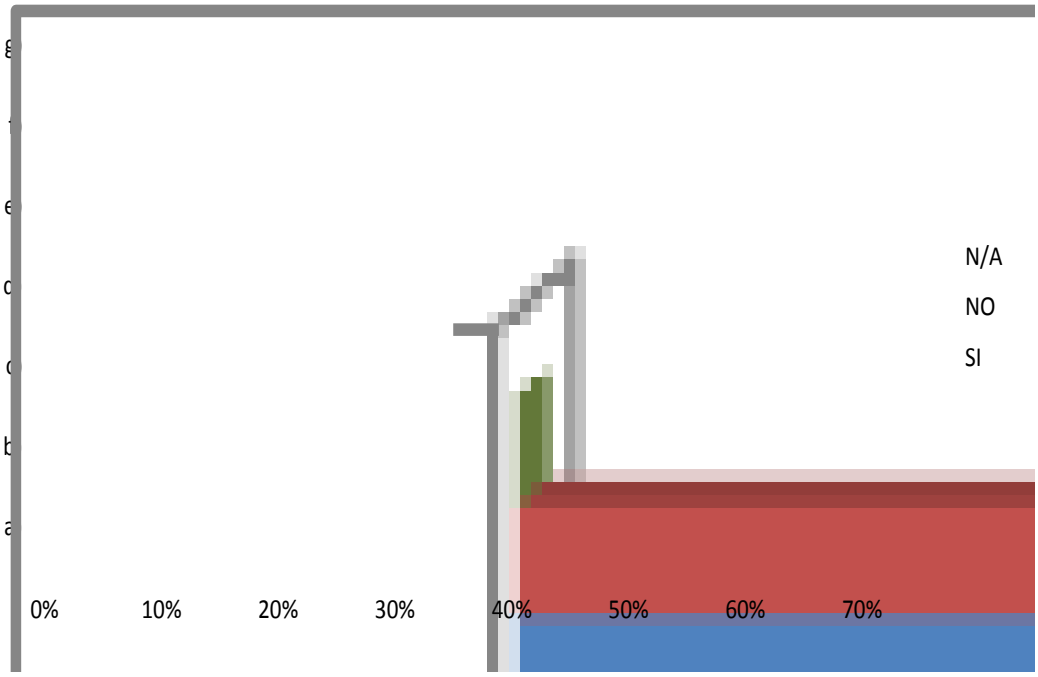
Como puede observarse en el gráfico, cuando se consultó en el ítem 1, sobre la necesidad de que se realicen revisiones periódicas a los sistemas de información, el 100% de los encuestados contesto afirmativamente, por lo que se infiere que se estima de gran importancia la revisión de los mismos, toda vez que el producto de esas revisiones contribuye a la buena marcha de la gestión empresarial.

Por otra parte cuando se les planteo en el ítem 2, si conocen alguna metodología de evaluación como la auditoría informática, el 70% respondió afirmativamente y un 30% negativamente, lo que indica que de

alguna manera el conocimiento de la auditoria informática evidencia la posible practica de dicha metodología, sin embargo se hace necesario una mayor divulgación y práctica de la misma.

Ítem 3

Dimensión: Aspectos que integran la metodología de Auditoría Informática.



Fuente: Cuestionario aplicado a expertos.

Tomando en consideración las respuestas de los ítems anteriores, se procedió a consultar algunos de los aspectos que podrían integrarse en la metodología de la Auditoria Informática, la muestra consultada respondió que sí debían incluirse los siguientes aspectos:

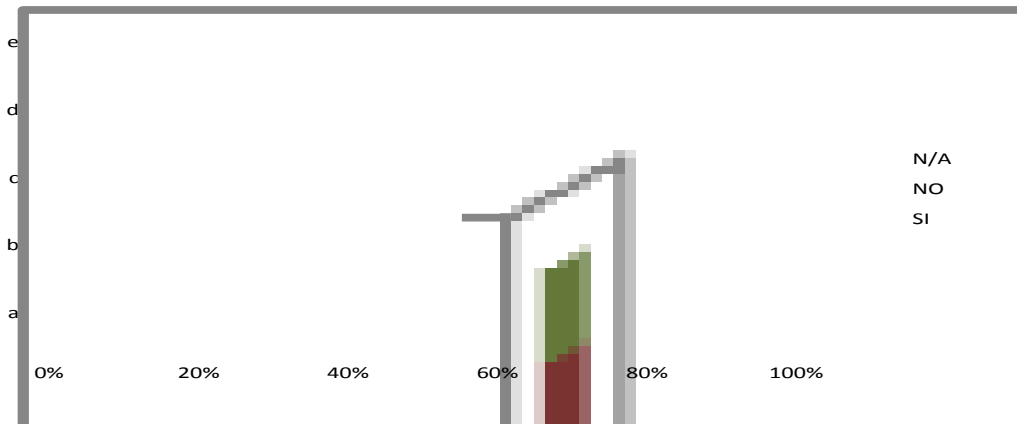
1. Alcance y Objetivos de la Auditoría Informática un 70%
2. Estudio inicial del entorno auditable un 60%

3. Determinación de los recursos necesarios para realizar la auditoría, un 70%
4. Elaboración del plan y de los Programas de Trabajo, un 70%
5. Actividades propiamente dichas de la auditoría, un 50%
6. Confección y redacción del Informe Final, un 50%
7. Redacción de la Carta de Introducción o Carta de Presentación del Informe final un 50%

En este sentido se evidencia un porcentaje de aceptación de los aspectos consultados, sin embargo es oportuno mencionar que un 10% opina que no es necesario realizar un estudio inicial del entorno auditable y un 20% piensa que no es necesario incluir las actividades propiamente dichas de la auditoria, confección y redacción del informe final, por lo que se estima que es necesario indagar sobre los aspectos relevantes de la metodología de auditoría informática y de que exista un Modelo a seguir para la práctica de la misma.

Ítem 4

Dimensión: Recursos de Auditoría Informática



Fuente: Cuestionario aplicado a expertos.

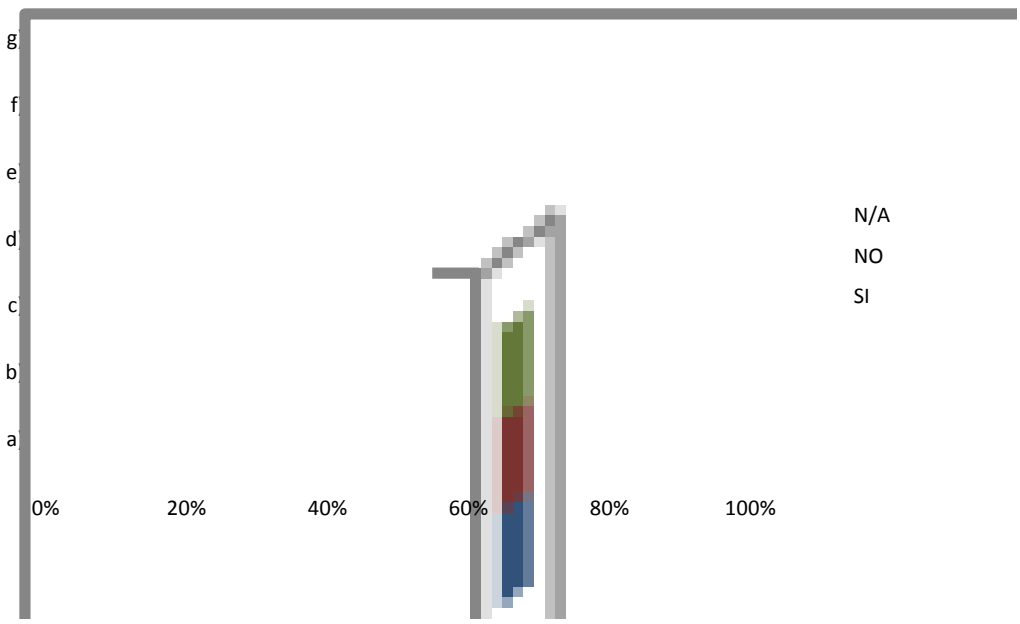
En cuanto a la consulta realizada sobre los recursos que se necesitan para realizar la auditoria informática las personas encuestadas respondieron de la siguiente forma:

1. Software, el 80% dice que si el 20% que no.
2. Hardware, el 70% dice que si el 30% que no.
3. Tiempo, el 100% dice que sí.
4. Personal, el 100% responde afirmativamente.
5. Otros sin opinión

Como puede observarse existe una buena aceptación de los recursos que se necesitan para practicar las auditorias informáticas.

Ítem 5

Dimensión: Técnicas de Auditoría Informática



Fuente: Cuestionario aplicado a expertos.

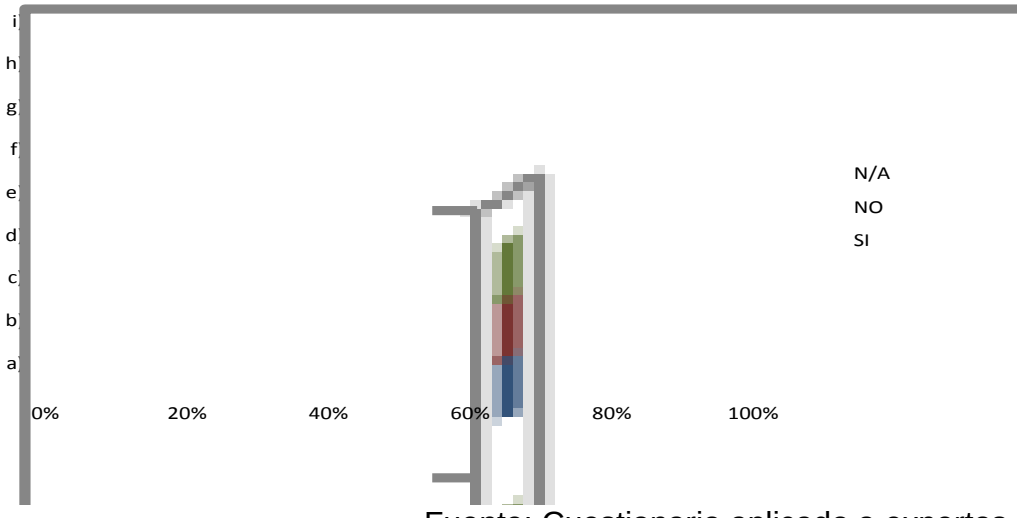
Al consultar sobre las técnicas que se necesitan para la aplicación de la Auditoria Informática, los encuestados opinaron lo siguiente:

1. Análisis de la información recabada del auditado, 100% responde afirmativamente.
2. Análisis de la información propia, 100% si.
3. Cruzamiento de las informaciones anteriores, 100% positivamente.
4. Entrevistas, 100% afirmativo
5. Simulación, 50% si y 50% no.
6. Muestreos, 70% si y 30% no
7. Otros que considere: no hubo opinión

Aun cuando hubo un buen porcentaje de aceptación a las técnicas de auditoría informática, puede decirse que es oportuno indagar sobre otras técnicas de apoyo a la función de la auditoria.

Ítem 6

Dimensión: Herramientas para la Auditoría Informática



Fuente: Cuestionario aplicado a expertos.

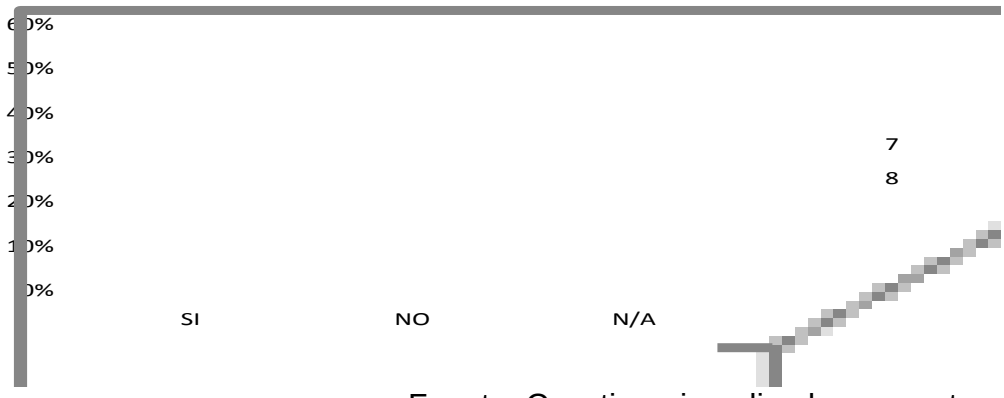
La muestra consultada opina en relación a las herramientas que necesita la auditoria informática lo siguiente:

1. Cuestionario general inicial, 50% si y 50% no.
2. Cuestionario, 100% si.
3. Checklist, 70% si y 30% no.
4. Estándares, 100% si.
5. Monitores, 70% si y 30% no.
6. Simuladores (Generadores de datos), 60% si y 40% no.
7. Paquetes de auditoría (Generadores de Programas), 70% si y 30%.
8. Matrices de riesgo, 100% si.
9. Otros que considere, sin respuesta.

Podemos inferir con estos resultados, que las herramientas propuestas tienen una buena aceptación para su uso al aplicar la auditoria informática, en este sentido es oportuno aplicarlas y buscar otras de apoyo.

Ítem 7 y 8

Dimensión: Conocimiento sobre la metodologías COSO y COBIT como apoyo a al control interno informático.

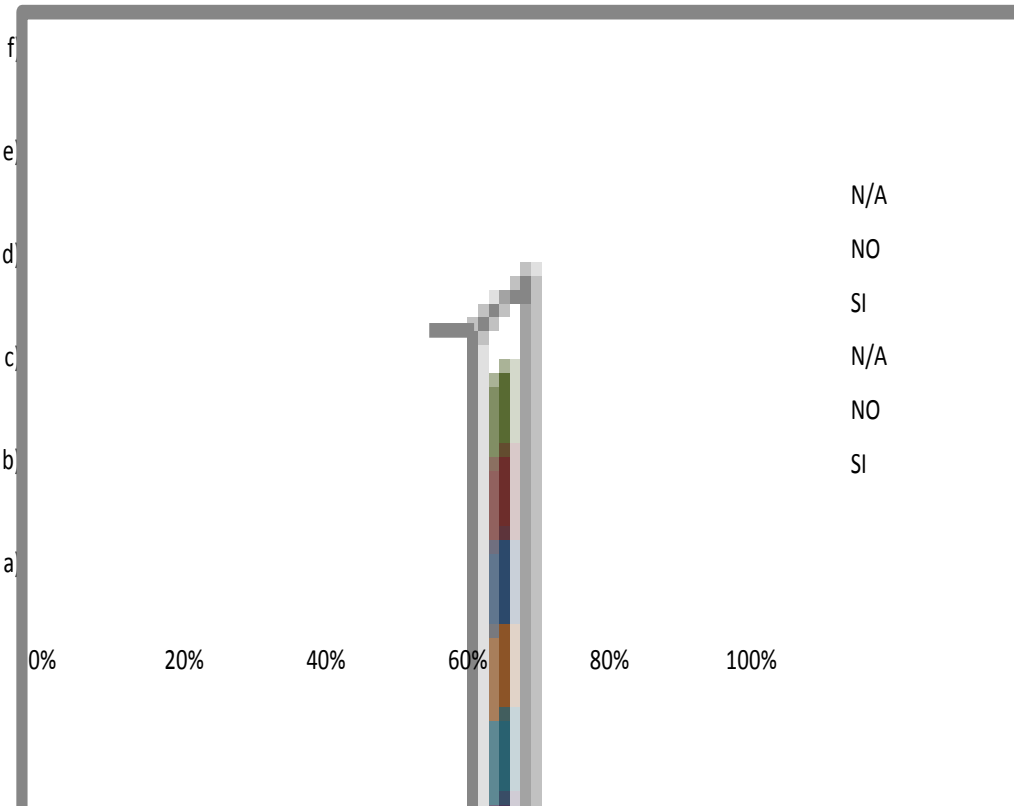


Fuente: Cuestionario aplicado a expertos.

Como puede evidenciarse en el gráfico, cuando fueron consultados los 7 y 8 conoce la metodología COSO y COBIT y si pueden servir de apoyo a la evaluación del control interno informático respectivamente, la muestra respondió para ambas preguntas en un 60% que si y 40% que no, lo que indica que dicha metodología es conocida, pero no del todo, por lo tanto como apoyo al control interno informático se hace necesario difundir dicha metodología, aplicarla y mostrar las ventajas en el uso de la misma.

Ítem 9

Dimensión: Áreas susceptibles para ser auditadas.

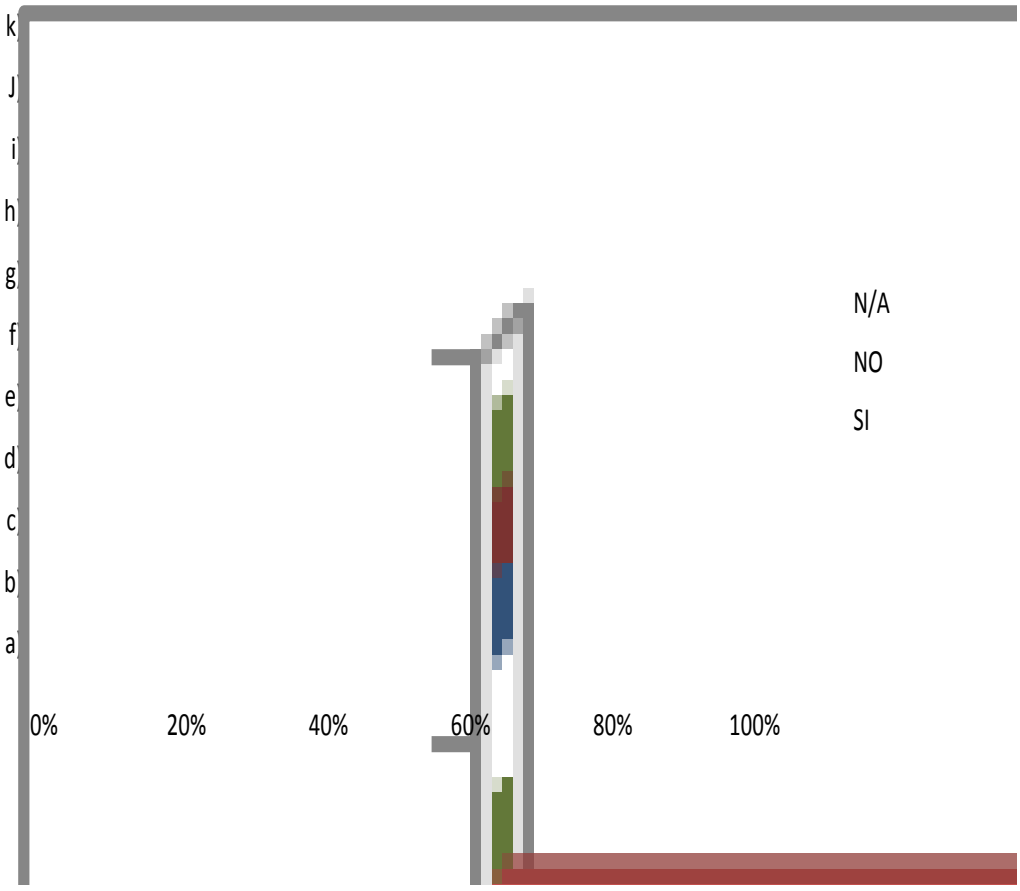


Fuente: Cuestionario aplicado a expertos.

Como se puede observar, en el grafico , el 100% de los encuestados respondió afirmativamente, indicando que las áreas susceptibles de ser auditadas son las siguientes: Base de Datos, Desarrollo de Software, Seguridad de la Información, Mantenimiento de aplicaciones y Redes, pudiendo inferirse que la realización de la auditoria informática puede extenderse a todo el entorno informático.

Ítem 10

Dimensión: Formación del Auditor Informático



Fuente: Cuestionario aplicado a expertos.

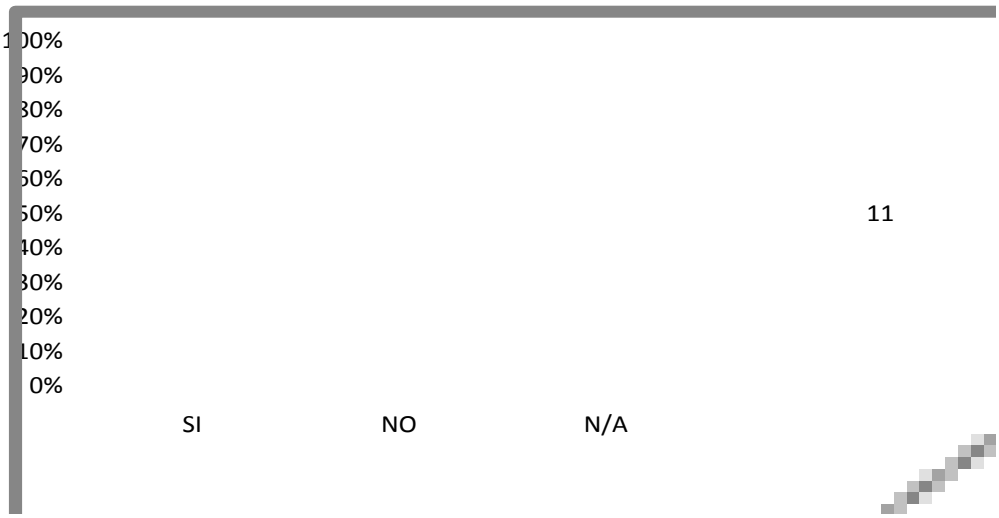
En lo que respecta, a la consulta realizada sobre la formación que debe poseer un auditor informático, los encuestados respondieron lo siguiente:

1. Desarrollo de software, 80% respondió afirmativamente y 20 % negativamente.
2. Gestión de proyectos de software, 70% si y 30% no.
3. Gestión y Análisis de riesgos en un entorno informático, 100% positivo.
4. Sistemas operativos, 70% si y 30% no.
5. Redes y Telecomunicaciones, 70% si y 30% no.
6. Gestión y administración de base de datos, 80% si y 20% no
7. Seguridad física, 100% si.
8. Operaciones e infraestructura informática, 100% si.
9. Gestión de la seguridad de los sistemas y de la continuidad empresarial a través de planes de contingencia, 100% si.
10. Gestión de problemas y cambios en entornos, 80% si y 20% no.
11. Otros, sin opinión.

Como puede inferirse por los resultados obtenidos, el auditor informático debe estar formado integralmente en todas las áreas de sistemas y tecnología de la información.

Ítem 11

Dimensión: Modelo de Auditoria Informática.



Fuente: Cuestionario aplicado a expertos.

Al consultar a los expertos si consideran necesario que las empresas, permitan la realización y aplicación de un Modelo de Auditoría Informática y evaluar así sus sistemas de información, en un 100% respondieron afirmativamente, lo cual indica la valoración e importancia que tiene la aplicación de la Auditoria Informática.

CAPITULO V

PROPUESTA

METODOLOGIA DE AUDITORÍA INFORMÁTICA PARA REVISAR LOS SISTEMAS DE INFORMACIÓN.

Presentación de la Propuesta

La Auditoría Informática es una actividad que ha cobrado fuerza en el campo de la Auditoría (que de forma tradicional se realizaba en el área financiera), con el incremento de la tecnologías de la información; la auditoría informática se expande a todas las áreas donde intervienen las tecnologías.

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.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Sus objetivos son: El control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos, la verificación del cumplimiento de la Normativa en este ámbito y la revisión de la eficaz gestión de los recursos informáticos.

Asimismo la auditoría informática sirve para mejorar ciertas características en la empresa como eficiencia, eficacia, rentabilidad y seguridad.

Generalmente se puede desarrollar la auditoria informática, en alguna o combinación de las siguientes áreas:

- Gobierno corporativo
- Administración del Ciclo de vida de los sistemas
- Servicios de Entrega y Soporte

- Protección y Seguridad
- Planes de continuidad y Recuperación de desastres

Para ello es necesario contar con lineamientos y herramientas estándares para el ejercicio de la auditoría informática, esto se ha promovido con la creación y desarrollo de mejores prácticas como COBIT, ISO, COSO e ITIL.

Por tanto una Metodología de auditoria informática, constituye una herramienta muy valiosa para guiar la práctica de la auditoria, en la evaluación de los sistemas de información de las organizaciones.

De allí la importancia de plantear una metodología de auditoría informática, para revisar los sistemas de información.

Fundamentación de la Metodología

La naturaleza especializada de la auditoría a los sistemas de información (SI), así como las destrezas necesarias para llevar a cabo tales auditorías, requiere de estándares que aplican específicamente a la auditoría de SI. Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (*Information Systems Audit and Control Association*®, ISACA®) es promover estándares aplicables internacionalmente para cumplir con su visión. El desarrollo y difusión de los Estándares de Auditoría de SI son una piedra angular de la contribución profesional de ISACA a la comunidad de auditoría. La estructura para los Estándares de Auditoría de SI brinda múltiples niveles de asesoramiento. En este sentido se pueden mencionar los tipos de estándares existentes, emitidos por ISACA (2005):

S1 El Estatuto de Auditoría

S2 Independencia

S3 Ética y Normas Profesionales

S4 Competencia Profesional

S5 Planeación

S6 Realización de labores de Auditoría

S7 Reporte

S8 Actividades de Seguimiento

S9 Irregularidades y Acciones Legales

S10 Gobernabilidad de TI

S11 Uso de la Evaluación de Riesgos en la Planeación de Auditoría

S12 Materialidad de Auditoría

S13 Uso del Trabajo de Otros Expertos

S14 Evidencia de Auditoría

S15 Controles TI

S16 Comercio Electrónico

Definición de la Metodología

La Metodología de Auditoria Informática para revisar los sistemas de información, se estructura con un conjunto de componentes mediante pasos a seguir para propiciar la transformación de la cultura organizacional, hacia la necesidad de revisar sus procesos y procedimientos en función de la evaluación de la integridad de sus sistemas, proporcionando a dichas organizaciones las recomendaciones necesarias para mantener una gestión eficaz y eficiente.

Misión de la Metodología

Brindar a las organizaciones, a través de la aplicación de la metodología de auditoria informática, información veraz y confiable, que les permita mantener la mejora continua de sus procesos, procedimientos y sistemas para la optimización del uso de la tecnología.

Visión de la Metodología

Consolidar la Metodología de Auditoria Informática para la revisión de los sistemas de información, como una estrategia preventiva, que forme parte

de la dinámica organizativa, proporcionado el conocimiento y las mejores prácticas en el diseño del control informático.

Filosofía de Gestión de la Metodología.

La filosofía de gestión de la presente metodología, se enmarca en valores que se integran en: Desempeño, Eficacia, Fiabilidad, Seguridad, Privacidad, honestidad, confianza, productividad, actitud abierta, enfocar al cliente, independencia, compromiso, que se traduce en trasparencia, creación de valor, cambio y servicio de calidad.

Desempeño

Realizar un examen objetivo, sistemático y profesional de evidencias, llevado a cabo con el propósito de hacer una evaluación independiente sobre la actuación de una entidad, programa o actividad, orientada a mejorar la efectividad, eficiencia y economía en el uso de los recursos humanos y materiales para facilitar la toma de decisiones.

Eficacia

Desarrollar la capacidad de alcanzar el efecto que se espera o se desea tras la realización de una acción, a través de la auditoria informática.

Fiabilidad

Analizar la probabilidad de que un sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período determinado.

Seguridad

Proporcionar a través de la auditoria informática, la protección de la confidencialidad, integridad y disponibilidad de los activos de información, para motivar que se alcancen los objetivos de negocio de la organización.

Privacidad

Asegurar la custodia de los papeles de trabajo, que tienen un carácter estrictamente personal.

Honestidad

Actuar con integridad, rectitud y apego a derecho, evitando la discrecionalidad en la toma de decisiones y la generación de conductas irregulares que afecten a las organizaciones auditadas.

Confianza

Garantizar seguridad y certeza en los auditores informáticos, respecto a la veracidad, objetividad, claridad, oportunidad y estricto apego a derecho en todos los actos que conlleven a la utilización de los hallazgos de auditoria informática.

Productividad

Realizar las actividades que contribuyan al uso de sus recursos en forma óptima e inteligente, que se reflejen en los resultados de las organizaciones sin detrimento de la calidad y oportunidad del servicio.

Actitud abierta

La apertura surge como una nueva estrategia, que genere confianza en el cliente.

Enfocar el cliente

Tratar a cada cliente individualmente y procurando proveerle exactamente el producto que necesita.

Independencia

Mantener la independencia de criterio, al momento de auditar a la organización y sus sistemas

Compromiso

La Metodología se fundamenta en la necesidad de que se cumpla consistentemente con los principios de la misión y valores para alcanzar resultados con los más altos estándares de desempeño.

Creación de valor

Al implantar y consolidar las redes de trabajo, este criterio es el elemento de contenido, y plantea el perfeccionamiento y reinicio de las cadenas de valor.

Cambio

A partir de un enfoque orientado a la satisfacción de necesidades, este criterio es el elemento dinámico, y reclama la innovación como factor de supervivencia y éxito.

Servicio de calidad

La intención fundamental de la Metodología es brindar a los clientes una atención de excelencia y con criterios de calidad sobre los procesos auditados en las organizaciones.

Objetivos de la Metodología

Objetivo general

Proporcionar los lineamientos básicos para desarrollar y orientar el proceso de Auditoria Informática para revisar los sistemas informáticos

Objetivos Específicos

1. Fomentar la aplicación de la Auditoria Informática, en las organizaciones, para que mantengan un proceso de evaluación activa de sus sistemas informáticos.
2. Presentar los procedimientos de auditoría informática necesarios, para la evaluación de los sistemas informáticos.
3. Proporcionar, las herramientas necesarias para el desarrollo y aplicación de la Auditoria Informática

Objetivos Estratégicos de la Metodología

1. Aplicar la Metodología de Auditoria Informática
2. Desarrollar los programas de divulgación de la Metodología de Auditoria Informática para estimular a las organizaciones a poner en práctica las auditorias informáticas de sus sistemas.
3. Formar en el área de Auditoria Informática, a los profesionales que lo requieran.

Justificación de la metodología

El activo más importante de una organización, sin duda, es su recurso humano y la información, por ende las empresas e instituciones invierten en la capacitación de la gente y en la tecnología, debido a que esto da valor agregado a la gestión de estas.

Esta Metodología está fundamentado en la necesidad de que las empresas, las instituciones, Universidades, etc. manejen procedimientos, para verificar que tan buenos son sus procesos con el uso de sistemas y tecnología, a fin de lograr los beneficios tangibles.

Asimismo a pesar de la existencia de metodologías para aplicar la Auditoria, la misma se ha orientado a las áreas contables, financieras, administrativas, fiscales, de gestión etc. de allí la necesidad de explotar el área de la informática, aplicando metodologías de la auditoria para evaluar

los sistemas en sus diferentes aspectos tales como base de datos, seguridad de la información, redes entre otras. Además esta metodología puede hacerse extensivo a las empresas e instituciones en general y llevarse a las universidades, para formar a profesionales mediante la enseñanza de la Auditoria Informática, como una herramienta que los puede ubicar en el campo de trabajo desde una perspectiva integral.

Componentes de la Metodología

La Metodología de Auditoria informática, para revisarar los Sistemas de Información, se construyó a partir de cuatro componentes:

Primer Componente: El Auditor y el Sistema de Información a auditar.

Puesto que se analiza a la organización y su sistema de información, a fin de reconocer el tipo de auditoría a desarrollar.

Segundo Componente: Procedimiento de Auditoria Informática.

La cual consiste en el diseño del Programa General y los Programas Específicos para auditar.

Tercer Componente: Aplicación del Procedimiento de Auditoria del Informática.

Es la aplicación del procedimiento en las Organizaciones, para medir los resultados y diseñar y presentar el informe respectivo.

Cuarto Componente: Sistema de Inversión para la Auditoria Informática

Consiste en la fijación de los medios para la delineación del sistema de inversión para la Auditoria Informática.

Operatividad de la metodología

Fase I. Sistema para la aplicación de la Metodología de Auditoria Informática.
Fase II. Sistema de Inversión para la Auditoria Informática

Fase III. Estrategias de Implantación de la Metodología de Auditoria Informática

Simulación de la metodología

Se simularon nueve (09) escenarios de auditoria informática que fueron presentados y analizados en el capítulo IV, de esta investigación

Estructura de la metodología

La presente Metodología se estructura de la siguiente manera:

1. PROCESO DE PLANIFICACIÓN DEL TRABAJO DE AUDITORIA INFORMÁTICA.

1.1. Definición del Equipo de Trabajo

El equipo de trabajo que realizará la auditoría informática, debe ser cuidadosamente seleccionado, puesto que el auditor desempeñara sus labores mediante la aplicación de una serie de conocimientos especializados que forman el cuerpo técnico de la actividad a ejecutar. El auditor adquiere responsabilidades, no solamente con la persona que directamente contratan sus servicios, sino con un número de personas desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones.

En este sentido la selección de los auditores, se hace con bases a las normas internacionales de auditoria informática promulgadas por ISACA, que establece en sus Normas personales, que “son cualidades que el auditor debe tener para ejercer sin dolo una auditoría, basados en un sus conocimientos profesionales así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias”. Asimismo su trabajo debe seguir los siguientes estándares:

- Cumplir con el Código de Ética Profesional de ISACA al realizar tareas de auditoría.

- Ejercer el debido cuidado profesional, lo cual incluye cumplir con los estándares profesionales de auditoría aplicables al realizar tareas de auditoría.
- Debe ser profesionalmente competente y tener las destrezas y los conocimientos para realizar la tarea de auditoría.
- Debe mantener competencia profesional por medio de una apropiada educación y capacitación profesional continua.

Por lo expuesto el equipo de trabajo estará conformado por un auditor encargado, líder o senior, un auditor supervisor y de más auditores asistentes u operativos, cuyo número dependerá de la magnitud de la auditoria informática a realizar. En resumen los auditores informáticos deberán cumplir lo siguiente:

Fuente: Adaptación de las Normas de Auditoria del Instituto Mexicano de Contadores Públicos.

1.2. Toma de Contacto con el cliente.

El equipo de auditoria enviará a uno o dos auditores, para entrevistarse con el cliente potencial, a los fines de reconocer no solo a la empresa a auditar, sino también determinar el alcance de la auditoria, de acuerdo al orden de prioridad de los requerimientos del cliente.

1.3. Determinación del Alcance de la Auditoria Informática

Una vez realizada la toma de contacto con el cliente y determinado los requerimientos del mismo, se plantea el alcance de la auditoria, en este se expresa: Empresa a auditar, tiempo necesario, tipo de auditoría informática a realizar, tipo de producto (software, redes, base de datos, etc.) a auditar según el caso.

1.4. Objetivos de la Auditoria Informática

Se definen los objetivos, general y específicos a demostrar en el trabajo de auditoria informática.

Solo se plantea un objetivo general. En lo que respecta a los objetivos específicos, pueden ser de cuatro a seis objetivos la cantidad va a depender del alcance de la auditoria. Para esto se puede seguir la siguiente pauta:

GENERAL “incluir el verbo de acción al alcance de la auditoría. Ejemplo: Realizar una Auditoría Informática de ……..”

Específicos: “Usar: Diagnosticar, evaluar el control interno informático, Analizar, Presentar informe.

1.5. Matriz de Análisis de la Auditoria Informática

A los fines de organizar el trabajo a seguir en la auditoria a realizar, es oportuno construir una matriz de análisis, de acuerdo a lo siguiente:

Matriz de Análisis Auditoria Informática

OBJETIVOS		Dimensión	Indicadores	Instrumentos
General	Específicos			

- En la columna de “Objetivos”, se identifica en una primera instancia en “General” la variable principal o variable dependiente, por Ejemplo: Auditoria Informática de Base de Datos, Auditoria Informática de Seguridad de la Información etc. Por otra parte en la columna de “Específicos”, se incluyen en forma resumida los objetivos específicos, tantos como existan.
- En la columna “Dimensión”, señale las variables independientes en función de los objetivos específicos, Ejemplo:
  Objetivo Específico: Diagnosticar la situación actual de la Gestión de la Base de Datos de…….
  Dimensión: Organización y Gestión.
- En la columna “Indicadores”, de acuerdo a cada dimensión, se identificaran los indicadores de medición cuantitativos y/o cualitativos, con la finalidad de valorar e indagar en el trabajo de auditoria.

- En la columna “Instrumentos”, se identificaran los instrumentos que servirán de apoyo al levantamiento de la información, los cuales serán diseñados de acuerdo al tipo de indagación de información que se quiere hacer, con la finalidad de obtener evidencias suficientes y competentes que den sustento al trabajo de la auditoria a realizar.

A continuación se presenta un ejemplo de una Matriz de Análisis de Auditoria Informática:

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La Auditoría es una necesidad en la actividad organizacional de nuestros tiempos, por lo que se vuelve imperiosa su aplicación para el logro de una efectiva evaluación de la funcionalidad de la misma, por tanto constituye una ventaja competitiva que las organizaciones la apliquen ya que les sirve de apoyo para ser eficaz y lograr niveles de eficiencia deseados.

Debido a la importancia que ha tomando el uso de los Sistemas de Información en el entorno empresarial, surge la necesidad de controlar su correcto uso, funcionamiento y seguridad, en este sentido la Auditoría Informática, resulta fundamental para lograr que dichos sistemas, sean confiables, seguros, sólidos, que cumplan con las leyes establecidas en materia informática y por tanto que exista una confianza en su uso.

Los sistemas de información proporcionan apoyo en diferentes contextos organizacionales y dan soporte al proceso de toma de decisiones y al servicio de los clientes de una empresa, por lo que evidentemente representan un factor crítico para cualquier organización.

Por tanto, la Auditoría Informática hoy día constituye un factor significativo para la sociedad, debido a la gran dependencia que las organizaciones tienen de sistemas que gestionen su información y ante la necesidad derivada de verificar la calidad de los servicios ofrecidos por estos sistemas de información, así como la de garantizar una adecuada seguridad que consista en una correcta confidencialidad, integridad y disponibilidad de los datos que gestionan, ya que son uno de los activos más importantes de las organizaciones.

Por otra parte, bajo las diferentes modalidades de Auditoría Informática que existen, se permite evaluar los sistemas de información en sus diferentes

contextos y se puede concluir lo siguiente de acuerdo a los casos especificados:

La Auditoría Informática de Dirección es una herramienta preventiva de los efectos negativos que ocasiona la mala coordinación, relación y la valuación de cada uno de los elementos que forman la gestión gerencial de la Organización. Su contribución permite a la Organización anticiparse ante las amenazas que se presentan.

La Auditoría Informática de Organización y Métodos, se persigue verificar la congruencia de los procedimientos documentados en función de la funcionalidad del principal sistema informático de la organización.

La Auditoría Informática de Desarrollo de SW, apoyo a las empresas desarrolladoras de software, evaluar el nivel de sus desarrollos en función de lo establecido en las Normas ISO 9000 y verificar el grado de congruencia del diseño con lo que establece la norma.

La Auditoría Informática de Base de Datos, evaluar la congruencia del método de diseño de la base de datos, en términos de los indicadores establecidos para tal fin.

La Auditoría Informática de Seguridad de la Información, permitirá evaluar los sistemas de información de acuerdo a los diferentes niveles de seguridad de la información, que van desde la seguridad lógica y física hasta inclusive la seguridad legal y organizacional, de acuerdo a lo establecido en la Norma ISO 27001 en vigencia.

La Auditoría Informática de Redes involucra la revisión de los tipos, arquitectura, topologías, protocolos, conexiones, accesos etc. por tanto constituye una herramienta que busca valorar todos los aspectos de la creación de las redes, su configuración, funcionamiento y aplicación, permitiendo analizar la forma en que las empresas aprovechan sus recursos informáticos.

La Auditoría Informática de Mantenimiento, pocos apunto a la aplicación de la misma, sin embargo en esta auditoría se evalúa el factor de calidad que

cubre todas las características del software, destinadas a lograr que el producto se más fácil de mantener, a fin de conseguir la mayor productividad en la fase de mantenimiento.

Auditoría Informática de Calidad, ayuda a comprende la revisión y análisis de los requisitos de funcionamiento y rendimiento del software, en concordancia con los estándares de desarrollo que han sido documentados, basado en las normas ISO 9000, específicamente desde la ISO 9001 a la ISO 9004 e ISO/IEC 9126, dirigida a la evaluación del producto de software

La diversificación y modalidades existentes de la Auditoría Informática, constituyen una herramienta poderosa para las organizaciones interesadas en la evaluación a sus sistemas informáticos, tanto desde el punto de vista físico como lógico.

Otro aspecto de interés para las organizaciones, la seguridad de la información, por tanto el análisis de los riesgos es directamente proporcional a la creación de un Sistema de Gestión de Seguridad de la Información (SGCI).

Se entiende la importancia que tiene la legislación existente en un país determinado y que sirve de apoyo a la realización de la Auditoría Informática, en este sentido es oportuno mencionar que en nuestro país Venezuela, existe legislación de apoyo entre las que se pueden mencionar: Decreto con Fuerza de Ley 1.204 sobre Mensajes de datos y Firmas Electrónicas, Ley Especial contra Delitos Informáticos, Ley de Tecnología de Información; Ley de Derechos de Autor y Autora, entre otras.

Es importante mencionar que independientemente del tipo de auditoría informática que se realice, se deben seguir leyes de apoyo, normas internacionales de auditoría y la metodología de trabajo apropiada y que propone los diferentes organismos internacionales que regulan en materia informática, tales como ISACA e ISO.

En lo que respecta a las principales pruebas a aplicar en una Auditoria Informática, son las pruebas sustantivas para verifican el grado de

confiabilidad del Sistema de Información de la empresa o institución, mediante la observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones, verificando asimismo la exactitud, integridad y validez de la información y las pruebas de cumplimiento para verificar el grado de cumplimiento de lo revelado mediante el análisis de la muestra, proporcionado evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Recomendaciones

Fomentar en las organizaciones, la aplicación de Auditorías Informáticas que les permitan evaluar la funcionalidad de sus sistemas informáticos, a fin de mantener la actualización constante de los mismos, lo cual servirá para mejorar ciertas características en la empresa como: Eficiencia, eficacia, rentabilidad y seguridad de la información.

Aplicar el Control Interno Informático con la finalidad de controlar que todas las actividades relacionadas a los sistemas de información automatizados se realicen cumpliendo las normas, estándares, procedimientos y disposiciones legales establecidas interna y externamente.

Se deben incentivar a las organizaciones para que posean un Sistema de Gestión de Seguridad de la información (SGSI) para que puedan reconocer los riesgos a los que está sometida su información y los gestionen mediante un sistema definido, documentado y conocido por todos su personal, y que debe revisarse y mejorarse constantemente. Asimismo deben aplicarse las Auditorías Informáticas de Seguridad de la Información.

Promocionar en las organizaciones la aplicación de la Metodología de Auditoría Informática para la revisión de los sistemas de información propuesto en la presente investigación.

OBJETIVOS		Dimensión	Indicadores	Instrumentos
General	Específicos			
Realizar una **auditoría informática de base de datos**, en la empresa XYZ., para el sistema de control de acceso de personal.	Diagnosticar la situación actual de la gestión de la base de datos del Sistema de Control de Acceso de Personal en la empresa XYZ.	Organización	❖ Existencia de documentación de objetivos. ❖ Existencias de políticas y normas en la empresa. ❖ Definiciones de cargos. ❖ Recursos humanos y materiales.	✓ Entrevistas. ✓ Cuestionarios. ✓ Observación ✓ directa.
		Gestión	❖ Segregación de funciones. ❖ Especificación de la plataforma y el lenguaje usado. ❖ Diccionario de Datos.	
	Evaluar las medidas de control interno y externo, para la base de datos del Sistema de Control de Acceso de Personal.	Calidad de los datos	❖ Integridad de datos. ❖ Consistencia de datos. ❖ Completitud de datos. ❖ Disponibilidad de datos.	✓ Observación directa. ✓ Entrevistas. ✓ Cuestionarios. ✓ Listas de Chequeo ✓ Pruebas de Software Caja Negra.
		Seguridad lógica	❖ Existencia de documentación de políticas de seguridad. ❖ Control de acceso. ❖ Gestión de archivos de auditoría LOGS. ❖ Existencia de documentación de políticas de respaldo y recuperación.	
	Analizar la información recolectada durante el proceso de auditoría informática de base de datos.	Análisis de la información	❖ Resultados obtenidos	
	Presentar informe del proceso de auditoría informática de base de datos.	Presentación del informe.	❖ Informe	

Fuente: Yépez (2010). Auditoria Informática de Base de Datos. Sistema de Control de Acceso de Personal.

1.6. Programa General de la Auditoria Informática

Para la realización del Programa General de Auditoria Informática, es muy importante detallar todas las actividades a realizar en cada fase de la Auditoria, para lo cual se sigue el siguiente esquema:

		Código:	
PROGRAMA GENERAL DE AUDITORIA INFORMATICA			
EMPRESA:		FECHA:	HOJA Nº DE
FASE	ACTIVIDAD	HORAS ESTIMADAS	ENCARGADOS
I	**Etapa Preliminar:** - Planificación de actividades. - Entrevista con el cliente - Levantamiento inicial de información - Definición de alcance y objetivos de la auditoría. - Elaboración de la matriz de análisis de auditoría. - Elaboración del programa de auditoría - Elaboración de los procedimientos de auditoría. - Elaboración de entrevistas - Elaboración de cuestionarios - Elaboración de pruebas de SW		
II	**Desarrollo de la Auditoria:** - Entrevistas con el personal objeto de Auditoría. - Aplicación de cuestionarios y listas de chequeo cuestionarios al personal objeto de auditoría. - Observación directa sobre los procesos auditados en la organización. - Recopilación de información y documentación relevante al proceso de Auditoría. - Análisis de la información recopilada y de ser necesario, utilizar herramientas automatizadas para la organización de los datos. - Determinación y tabulación de resultados (Hallazgos, observaciones, recomendaciones y conclusiones).		
III	**Revisión y Pre-Informe** **-** Revisión general de los resultados. - Elaboración del Pre-Informe.		
IV	**Informe** - Elaboración de informe final. - Presentación del informe.		

Fuente: Camacaro (2009).

2. Sistema de Inversión para la Auditoria Informática.

2.1. Definición de Cadena de Valor

a) Definir el Presupuesto Estimado para la Auditoria Informática

Con base a lo detallado en el Plan General de la Auditoria Informática, el alcance y los objetivos, se procede a la estimación de las horas de trabajo

El equipo de auditoria estimará, las horas necesarias del trabajo de auditoria, considerando el grado de participación de cada uno de los integrantes del equipo de trabajo en función de las actividades que realiza, para ello pudiera seguirse los siguientes pasos:

- Definir en términos porcentuales y de acuerdo a la estructura de cargos del equipo de trabajo, su participación en el trabajo a realizar, por Ejemplo:

DISTRIBUCION PORCENTUAL DEL TIEMPO DE TRABAJO

CATEGORIA	% DE TIEMPO DE TRABAJO
SOCIO	5
GERENTE	5
SUPERVISOR	10
ENCARGADO O SENIOR	15
SEMI-SENIOR	15
ASISTENTES	45
OTROS	5
TOTAL	**100**

Fuente: Elaboración propia.

Dicha distribución de trabajo se modificará a criterio del equipo de trabajo de la auditoria.

- Una vez definido el porcentaje de participación, se procederá a la distribución de horas desglosando las actividades a realizar de la siguiente forma:

Empresa XYZ
Propuesta de Servicios para Auditoria Informática

Personal /Actividades	Socio	Gerente	Supervisor	Senior	Semi-Senior	Asistente	Asistente	Otros	TOTAL
Información General									
Planificación									
Elaboración de Cuestionario C.I									
Evaluación del Control Interno									
Elaboración de Programas de Auditoria									
Identificación de Riesgos									
Identificación de Controles									
Aplicación de Pruebas									
Evaluación de los Sistemas de Información									
Revisión de los Papeles de Trabajo.									
Elaboración del Informe									
Discusión del Informe									
Entrega y Presentación Final									

Fuente: Elaboración propia.

El formato anterior, será sometido a las variaciones necesarias, de acuerdo a los criterios establecidos por la empresa o institución auditora.

a) Diseñar Estrategias Internas

Estas estrategias deben orientarse a:

- La Organización
- Al producto a auditar
- Precio
- Distribución
- Comunicación
- Tecnología de Información
- Personal
- Cartera de Clientes

b) Identificar las Bases para competir

- Desarrollo de Competencias
- Capacidades
- Activos Tangibles e Intangibles
- Sinergia en el equipo de trabajo para la buena atención del Cliente.
- Productos de la Auditoria Informática

3. Estrategias para la ejecución de la Metodología

Planificación

El proceso de planificación para la ejecución del trabajo de la auditoria informática, se completa, con el desarrollo de la planificación previa (Toma de Contacto, Alcance, Objetivos, matriz de análisis de la auditoria y el programa general de la auditoria), unido a la elaboración de los programas específicos (Procedimientos de Auditoria), la estimación de las horas de auditoria, presupuesto y el cronograma de trabajo.

Ejecución

Durante el proceso de ejecución, se elaboraran los instrumentos necesarios, para el levantamiento de la información y la aplicación de pruebas, para así obtener las evidencias que apoyen lo hallazgos de auditoria y sustenten las conclusiones y recomendaciones.

Los instrumentos a aplicar, pueden ser entrevistas estructuradas, cuestionarios, listas de chequeo, matriz de riesgos, matriz de análisis de contenidos, pruebas de caja negra o de caja blanca al sistema entre otros, asimismo la aplicación de las diferentes metodologías existentes, tal es el caso de la metodología COBIT, para la evaluación del control interno informático, ISO 27000, para la auditoria de Seguridad de la Información, técnicas de muestreo, técnicas de análisis y tabulación de resultados y otras que han sido descritas a lo largo de la presente investigación.

Revisión y Pre-Informe

Durante esta fase se realiza una revisión general de los resultados obtenidos del desarrollo de la auditoria, para proceder a realizar un pre-informe o borrador del informe final.

Informe

El informe de auditoría informática se entrega un vez que ha finalizado el trabajo de auditoria, tomando en consideración las revisiones y ajustes necesarios que considere el auditor líder. Dicho informe puede estructurarse de la siguiente manera:

INFORME DE AUDITORIA

1. Identificación del informe
2. Identificación del Cliente
3. Identificación de la Entidad Auditada
4. Alcance de la Auditoria
5. Objetivos
6. Hallazgos de Auditoria
7. Conclusiones
8. Recomendaciones
9. Fecha del Informe

	Planificación	Ejecución	Informe
Fechas	xx/xx/xx al xx/xx/xx	xx/xx/xx al xx/xx/xx	xx/xx/xx al xx/xx/xx

10. Identificación y Firma del Auditor

Apellidos y Nombres	Cargo

Fuente: Elaboración Propia.

Cuestionario de control interno

Auditoría informática de dirección

ITEMS	SI	NO	N/A
1. La Dirección de Informática desarrolla planes a corto, mediano y largo plazo que apoyen el logro de sus objetivos ?			
2. La Dirección de Informática dispone de un Plan Estratégico de Tecnología de la Información ?			
3. En el proceso de planificación se presta atención a los establecido en el Plan Estratégico ?			
4. Los recursos asignados son suficientes para llevar a cabo las tareas y actividades establecidas en la planificación ?			
5. El espacio físico existente en el lugar de trabajo es adecuado ?			
6. Los equipos existentes están acordes con la tecnología actual ?			
7. Se cuenta con el personal suficiente para la realización de todas actividades de la Dirección de Informática ?			

Cuestionario de control interno
Auditoría informática de seguridad física

ITEMS	SI	NO	N/A
1. Adopción de medidas de seguridad en el área física	X		
2. Existencia de persona responsable de la seguridad	X		
3. División de responsabilidad en cuanto la responsabilidad	X		
4. Existencia de Vigilancia en el área		X	
5. Servicio de Vigilancia Contratado	X		
6. Acceso permitido a cualquier persona	X		
7. Existencia de Salida de Emergencia		X	
8. Existencia de Control de Acceso al Departamento		X	
9. Detector de Incendios		X	
10. Alarmas		X	
11. Adiestramiento al personal para manejo de extintores		X	
12. Adecuación de Aires Acondicionados	X		
13. Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos.		X	
14. Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo		X	
15. Se limpia con frecuencia el polvo acumulado	X		
16. Hay bloqueos y procedimientos de entrada para obtener acceso a los servidores	X		
17. Hay protección contra el robo de hardware	X		
18. Se guardan los paquetes y licencias de software y las copias de seguridad en lugares seguros	X		
19. Hay procedimientos para almacenar los datos, copias de seguridad y software con licencia en las instalaciones y fuera de ellas	X		
20. Existe departamento de auditoría interna en la institución		X	
21. Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computación.	X		

Cuestionario de control interno

Auditoría informática de seguridad lógica y física

1. Utiliza usted la RED-UCLA ?
   i. SI_____ NO_____
2. Recibió usted alguna inducción para el uso y manejo de los servicios de la RED-UCLA ?
   i. SI_____ NO_____
3. Con que fin la usa ?
   1. Investigación _____
   2. Administrativo _____
   3. Académico _____
   4. Comunicación _____
   5. Pasatiempo _____
4. Cual usa más frecuentemente ?
   1. Investigación _____
   2. Administrativo _____
   3. Académico _____
   4. Comunicación _____
   5. Pasatiempo _____
5. Utiliza usted el correo de la UCLA ?
   i. SI_____ NO_____
6. Se ve afectada su cuenta de correo por el SPAM ?
   i. SI_____ NO_____
7. Está conforme con la velocidad de conexión de la RED-UCLA ?
   i. Si_____ NO_____
8. Utiliza RED-UCLA para revisar cualquiera de sus cuentas de correo electrónico ?
   i. Si_____ NO_____
9. Que tipo de datos descarga usualmente en la RED-UCLA ?
   i. Programas _____
   ii. Trabajos académicos _____
   iii. Documentos _____
   iv. Presentaciones _____
   v. Juegos _____

vi. Música _____
vii. Videos _____

10. Como describe el rendimiento de la RED-UCLA ?
    i. Excelente _____
    ii. Bueno _____
    iii. Moderado _____
    iv. Malo _____
11. Que tipo de equipo utiliza para acceder a la RED-UCLA ?
    i. PC _____
    ii. Centro de computación _____
    iii. Laptop _____
12. Chequea usted con un antivirus los medios de almacenamiento como Pendrive o CD antes de utilizarlos ?
    i. Nunca _____
    ii. A veces _____
    iii. Siempre _____
13. Cada cuanto tiempo actualiza usted su antivirus ?
    i. Semanalmente _____
    ii. Mensualmente _____
    iii. Anualmente _____
    iv. Nunca _____
    v. A veces _____
    vi. No aplica _____
14. Conoce usted de la existencia de normas de seguridad informática y de telecomunicaciones de la UCLA ?
    i. SI_____ NO_____

15. Conoce usted de las sanciones que podrían aplicarle por incumplimiento de las leyes ?
    i. SI_____ NO_____

16. Esta consciente que puede ser sancionado por acciones fraudulentes en la RED . Cuales conoce?
    i. Acceso a páginas impúdicas _____
    ii. Uso indebido de email _____
    iii. Uso indebido de extensiones telefónicas _____
    iv. No cree que pueda ser sancionado _____
    v. Asignación no autorizada de direcciones IP _____

Cuestionario de control interno

Auditoría informática de seguridad

Semestre que cursa ?

1º ____

2º ____

3º ____

4º ____

5º ____

6º ____

7º ____

8º ____

9º ____

ITEMS	SI	NO	N/A
1. ¿Conoce las normas y reglamentación de uso de las áreas y los equipos informáticos?			
2. ¿Considera que el software y las políticas de seguridad vigentes son suficientes para garantizar la protección e integridad de los equipos?			
3. ¿Existe difusión de las normas y políticas de seguridad del Centro de Computación?			

Cuestionario de control interno

Auditoría informática de seguridad

Usted se desempeña como ?

Preparador _____ Ayudante de Soporte Técnico _____

ITEMS	SI	NO	N/A
1. ¿Conoce reglamentación y políticas de seguridad para laborar en CCDCYT?			
2. ¿Existe difusión de las normas y políticas de seguridad del Centro de Computación?			
3. ¿Cree que los controles de acceso al sistema y a los recursos informáticos; son suficientes para evitar intrusiones, daños o actividades no autorizadas?			
4. ¿Cree que los controles de acceso al sistema y a los recursos informáticos; son suficientes para evitar intrusiones, daños o actividades no autorizadas?			

ENTREVISTA

Auditoría Informática de Base de Datos

1. ¿Conoce Ud. los objetivos generales y específicos de la organización?

2. ¿Considera Ud. que están debidamente establecidos los objetivos generales y específicos de la organización?

3. ¿Existe un organigrama donde se defina claramente la estructura organizacional de la Empresa?

4. ¿De existir dicho organigrama, considera Ud. que está disponible y observable fácilmente por todo el personal?

5. ¿Considera Ud. que están claramente definidas y documentadas las políticas y normas organizacionales?

6. ¿Piensa Ud. qué el personal conoce y aplica las políticas y normas organizacionales?

7. Considera Ud. que están bien definidos y documentados los cargos y funciones dentro de la organización?

8. ¿Piensa Ud. que el sistema de control de acceso de personal se alinea con los objetivos de la organización?

9. ¿Piensa Ud. que la plataforma tecnología actual permite el uso efectivo, eficiente y seguro del Sistema de Control de Acceso de Personal?

10. ¿Existe un personal designado para la gestión de la base de datos del Sistema de Control de Acceso de Personal?

11. ¿Considera Ud. que el personal asignado para la gestión de la base de datos está capacitado para realizar dicha labor?

ENTREVISTA

Auditoría Informática de Base de Datos

1. ¿Qué opina sobre la plataforma tecnológica actual para la gestión del sistema de control de acceso de personal?

2. ¿Considera que la plataforma tecnológica del sistema de control de acceso de personal se adapta a las necesidades actuales de la organización?

3. ¿Cree necesario la incorporación de nueva tecnología, para optimizar el funcionamiento del sistema de control de acceso de personal?

4. ¿Qué tan bien conoce Ud. el Sistema de Gestión de Base de Datos usado por el Sistema de Control de Acceso de Personal?

5. ¿Cree Ud. que el administrador de base de datos se ve afectado por la información almacenada en el sistema de Control de Acceso de Personal?

6. ¿Existe un diccionario de datos? ¿De existir, considera Ud. que se mantiene actualizado?

Cuestionario de Control Interno

Auditoría de Base de Datos

Preguntas	SI	NO
1. ¿Aplica Ud. alguna metodología o técnica para el diseño de la base de datos?		
2. ¿Usa alguna herramienta automatizada o aplicación para el diseño de la base de datos?		
3. ¿Aplica Ud. algunas de las formas normales estipuladas por el proceso de normalización de base de datos?		
4. ¿Están identificadas y documentadas las tablas maestras de la aplicación?		
5. ¿Están identificadas y documentadas las tablas o datos que son de carácter histórico?		
6. ¿Están identificadas y documentadas las tablas de transacción?		
7. ¿Está definida y documentada la cardinalidad en las relaciones entre las tablas?		
8. ¿Aplica la eliminación lógica de Datos para todas las tablas en la base de datos?		
9. ¿Se validan los datos al realizar una eliminación de un registro que afecta a otros registros en otras tablas?		
10. ¿Existe consistencia entre la información ingresada en el sistema y la información almacenada en la base de datos?		
11. ¿Existe validación a nivel de formularios para el ingreso de la información?		
12. ¿Se utilizan transacciones al realizar operaciones de almacenado de datos?		
13. ¿Se utilizan “ROLLBACK” para operaciones fallidas en el sistema de control de acceso de personal?		
14. ¿Se utilizan “COMMIT” para asegurar que la información está en la base de datos tras una operación satisfactoria?		

Cuestionario de Control Interno

Auditoría Informática de base de Datos

Preguntas	SI	NO	N/A
1. ¿Es suficiente la información brindada por el sistema de control de acceso de personal para realizar sus labores?			
2. ¿Cree Ud. necesario la incorporación de mayor información al sistema para facilitar la realización de sus labores?			
3. ¿Confía Ud. en la información arrojada por el sistema?			
4. ¿Durante su uso, el sistema de control de acceso de personal ha arrojado información errónea o incoherente, ocasionando problemas en el desempeño de sus funciones?			
5. ¿Tiene acceso a la información que necesita aun si el sistema está siendo accedido por otros usuarios al mismo tiempo?			
6. ¿Ha presentado problemas de desempeño durante la realización de alguna operación en el sistema de control de acceso de personal, afectando sus funciones en la organización?			
7. ¿Ha tenido problemas en acceder a la información necesaria para cumplir sus funciones debido a restricciones de seguridad?			
8. ¿Puede generar reportes impresos con la información que necesita para desempeñar sus labores de la manera más óptima?			

Auditoría Informática de Base de Datos

Tipo de Documento:	Lista de Chequeo	

Objetivo:
- Identificar las políticas, normas de seguridad, gestión de respaldo y recuperación existentes en la organización para la gestión de la base de datos del sistema de control de acceso de personal.

Forma de uso: Marque con ✓na en el recuadro si se cumple la característica chequeada, en caso contrario relleno con una X e indique cualquier observación relevante.

Auditor:		Fecha	

Características a chequear

☐ 1. Control de acceso a nivel de base de datos
Observ._____
_____
_____
_____

☐ 2. Documentación de los perfiles de seguridad por los cuales se tendrá acceso a la base de datos
Observ._____
_____
_____
_____

☐ 3. Plantillas de perfiles de seguridad (scripts) definidas para la creación de usuarios en la base de datos
Observ._____
_____
_____
_____

☐ 4. Control de acceso a nivel de la aplicación
Observ._____
_____
_____
_____

☐ 5. Abstracción de la información mediante vistas para el usuario
Observ._____
_____
_____
_____

☐ 6. Validación y Manejo de errores en la entrada de datos
Observ._____
_____

_____
_____

☐ 7. Claves de usuarios encriptadas
Observ._____
_____
_____
_____

☐ 8. Metodología para la recuperación y cambio de contraseñas a nivel de aplicación
Observ._____
_____
_____
_____

☐ 9. Protección de la información sensible para los usuarios y la organización
Observ._____
_____
_____
_____

Tipo de Documento:	**Lista de Chequeo**	

Objetivo:
- Identificar las políticas, normas de seguridad, gestión de respaldo y recuperación existentes en la organización para la gestión de la base de datos del sistema de control de acceso de personal.

Forma de uso: Marque con ✓na en el recuadro si se cumple la característica chequeada, en caso contrario relleno con una X e indique cualquier observación relevante.

Auditor:		Fecha	

Características a chequear

☐ 10. Reporte de acceso al sistema a nivel de la aplicación
Observ._____
_____
_____
_____

☐ 11. Rastreo de responsable y fecha de modificación de registros para tablas maestras
Observ._____
_____
_____
_____

☐ 12. Respaldos periódicos de la base de datos
Observ._____
_____
_____
_____

☐ 13. Planes de acción en caso de violaciones a las medidas de seguridad de la base de datos
Observ._____
_____
_____
_____

☐ 14. Definición y documentación de los períodos de almacenamiento de datos de respaldo
Observ._____
_____
_____
_____

☐ 15. Existencia de personal encargado de gestionar los respaldos de base de datos
Observ._____
_____
_____
_____

☐ 16. Plan de gestión para el control de los archivos de auditoría LOG
Observ._____
___
_____
__

☐ 17. Existencia de personal encargado de gestionar el control de los archivos de auditoría LOG
Observ._____
___
_____
__

CUESTIONARIO

No.	PREGUNTAS	SI	NO	N/A
1.	¿Considera necesario que se realicen revisiones periódicas a los sistemas de información en las Empresas?			
2.	¿Conoce usted alguna metodología de trabajo de evaluación a los sistemas de información como la de auditoría informática?			
3.	Si la respuesta anterior es afirmativa, señale si considera oportuno que las etapas que se señalan a continuación integren dicha metodología de Auditoria Informática: ▪ Alcance y Objetivos de la Auditoría Informática ▪ Estudio inicial del entorno auditable ▪ Determinación de los recursos necesarios para realizar la auditoría ▪ Elaboración del plan y de los Programas de Trabajo ▪ Actividades propiamente dichas de la auditoría ▪ Confección y redacción del Informe Final ▪ Redacción de la Carta de Introducción o Carta de Presentación del Informe final.			
4.	¿Qué tipo de recursos necesita una auditoría Informática? ▪ Software. ▪ Hardware. ▪ Tiempo. ▪ Personal. ▪ Otros que considere:_____ _____			
5.	Señale cuales de las técnicas en referencia pueden apoyar el trabajo de Auditoria Informática: ▪ Análisis de la información recabada del auditado ▪ Análisis de la información propia ▪ Cruzamiento de las informaciones anteriores ▪ Entrevistas ▪ Simulación ▪ Muestreos ▪ Otros que considere:_____ _____			

6.	¿Pueden las siguientes herramientas apoyar a la Auditoria Informática?: ▪ Cuestionario general inicial ▪ Cuestionario ▪ Checklist ▪ Estándares ▪ Monitores ▪ Simuladores (Generadores de datos) ▪ Paquetes de auditoría (Generadores de Programas) ▪ Matrices de riesgo ▪ Otros que considere:_____ _____			
7.	¿Las metodologías señaladas a continuación apoyan a la evaluación del Control Interno Informático?: ▪ COSO ▪ COBIT ▪ Otros que considere:_____ _____			
8.	¿Cuál de las siguientes áreas son susceptibles para ser auditadas?: ▪ Base de Datos ▪ Software ▪ Seguridad de la Información ▪ Aplicaciones ▪ Redes ▪ Otros que considere:_____ _____			

9.	¿Qué formación cree debería poseer un Auditor Informático?: ▪ Desarrollo informático. ▪ Gestión de proyectos de desarrollos, ▪ Gestión del Departamento de Sistemas Análisis de riesgos en un entorno informático, ▪ Sistema operativo, ▪ Telecomunicaciones, ▪ Gestión de base de datos ▪ Redes locales. ▪ Seguridad física, ▪ Operaciones y planificación informática, ▪ Gestión de la seguridad de los sistemas y de la continuidad empresarial a través de planes de contingencia de la informática, ▪ Gestión de problemas y de cambios en entorno informático. ▪ Administración de datos. ▪ Otros que considere:_____ _____			
10.	¿Considera necesario que las empresas, permitan la realización y aplicación de un Modelo de Auditoria Informática y evaluar así sus sistemas de información?			

ANEXOS

ANEXO A

REFERENCIAS BIBLIOGRAFICAS.

AMBROSÍ, A. y Otros (2005). **Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información**publicado por C & F Éditions. Sally Burch

AGENCIA NACIONAL DE EVALUACIÓN DE CALIDAD Y ACREDITACIÓN (ANECA). (2004). **Libro Blanco Título de Grado en Ingeniería Informática**.Universidad Politécnica de Catalunya. España.

ALONSO, CATALINA M., et. al. (2000). **"Los Estilos de aprendizaje. Procedimientos de diagnóstico y mejora".**Ediciones Mensajero: Bilbao.

ALFONSO S., ILIANA. (2004). **Elementos conceptuales básicos del proceso de enseñanza-aprendizaje.** Red Telemática de Salud en Cuba (Infomed). Calle 27 No. 110 e/ M y N. El Vedado. Plaza de la Revolución.Ciudad de La Habana, Cuba. [Documento en Línea]. Disponible:http:bvs.sld.cu/revistas/aci/vol11_6_03/aci17603.htm - 29k [Consulta: 2006, Septiembre 20]

ANEAS A., AASSUMPTA. (2003). **Competencias Profesionales. Análisis Conceptual y Aplicación profesional.** Extracto de conferencia presentada en el Seminario Permanente de Orientación Profesional, organizado por el Departamento de Métodos de Investigación y Diagnóstico en Educación. Universidad de Barcelona.

BARRIOS, M. Y OTROS (1998). **Manual de Trabajos de Grado de Especialización y Maestrías y Tésis doctorales.** Caracas: Editorial UPEL.

BOLETIN DE NORMAS Y PROCEDIMIENTOS DE AUDITORIA: Comité de procedimientos de auditoría, Instituto Mexicano de Contadores Públicos. 2009

BRUNER Y MELLER (2003). **Competencias profesionales y técnicas en la sociedad del conocimiento.** Hipertexto de la Universidad de Chile. Publicado por el Ministerio de Educación de Chile. [Documento en Línea]. Disponible:http://www.futurolaboral.cl/FL/biblioteca/.[Consulta: 2006, Febrero 20]

BUNK, G. P., (1994) **La transmisión de las competencias en la formación y perfeccionamiento profesionales en la RFA**, Revista CEDEFOP Nº 1.[Documento en Línea]. Disponible:http://dialnet.unirioja.es/servlet/articulo?codigo=131116. [Consulta: 2006, Marzo 03]

CASA, MIGUEL (2005) Nueva Universidad ante la sociedad del conocimiento. Revista de Universidad y Sociedad (RUSC) Vol.2 , Núm. 2, 2005 (enlace a www.uoc.edu/rusc/).

CAVANDES (2002) Auditoría Informática, disponible : http://www.monografías.com/trabajos/auditoinfo/auditoinfo.html

CARRIZO, L. (2004).**CONOCIMIENTO Y RESPONSABILIDAD SOCIAL Retos y Desafíos hacia la Universidad Transdisciplinaria.**DIÁLOGO GLOBAL LA RESPONSABILIDAD SOCIAL UNIVERSITARIA Iniciativa Interamericana de Capital Social, Ética y Desarrollo del BID Red Global de Aprendizaje para el Desarrollo.[Documento en Línea]. Disponible: http.controlinterno.udea.edu.co/docs/proyrsu/doc_interes/cono-cimiento.[Consulta: 2006, Abril 25]

COLL, C. **"Constructivismo e intervención educativa"**. **En: El constructivismo en la práctica**, España, Editorial Laboratorio educativo, 2000.

COMUNIDAD VIRTUAL DE INTERÉS DOCENTE. (2004). **Estilos de aprendizaje y perspectivas de la enseñanza. Reflexión sobre los estilos de Aprendizaje y las perspectivas de enseñanza.**Universidad Popular Autónoma del Estado de Puebla. (UPAEP).México.[Documento en Línea]. Disponible: http://www.upaep.mx/Biblioteca/Comunidad4.htm.[Consulta: 2006, Abril 02]

CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. (2000). Publicada en Gaceta Oficial Extraordinaria N° 5.453 de la República Bolivariana de Venezuela. Caracas, Marzo 24, 2000.

COMITÉ DE NORMAS INTERNACIONALES DE CONTABILIDAD. 2004. Normas Internacionales de Contabilidad.

COMITÉ OF SPONSORING ORGANIZATIONS OF TREADWEY COMMISSION (COSO). 1999. Control Interno Estructura Conceptual Integrada. Editorial ECOE. Bogotá, Colombia

Consejo superior de informática del Ministerio de Administraciones Públicas de España MARGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) 1997.

COOPERS & LYBRAND. 1997. Los Nuevos Conceptos del Control Interno Informe COSO. Díaz de Santos. España.

DE AGUSTÍN MELENDRO, Juan Antonio. 1995. Aplicación del Muestreo Estadístico a la Auditoria. Registro de Economistas Auditores (REA). Primera Edición. Madrid (España).

DOCUMENTOS SOBRE LA CUMBRE MUNDIAL SOBRE LA SOCIEDAD DE LA INFORMACIÓN (CMSI), desarrollada en dos fases; en Ginebra, del 10

al 12 de diciembre de 2003, y en Túnez, del 16 al 18 de noviembre de 2005.

DÍAZ, F. Y HERNÁNDEZ G. (1998). **Estrategias Docentes Para un Aprendizaje Significativo. Una Interpretación Constructivista.** México: Editorial Mc Graw-Hill.

ELLIOT , J. (1994). **La investigación-acción en educación**. Madrid: Morata.

FEDERACIÓN DE COLEGIOS DE CONTADORES PÚBLICOS DE VENEZUELA. 2002. Declaraciones de Normas de Auditoria (DNA), Publicaciones Técnicas (PT) y Servicios Especiales prestados por Contadores Públicos (SECP), de Aceptación General en Venezuela. Tomo II. Fondo Editorial del Contador Público Venezolano. Quinta Edición. Venezuela.

GONZALES S., S. (2006). **Un modelo BlendedLearning para la enseñanza de la Educación Superior.**Universidad Inca Garcilaso de la Vega[Documento en Línea]. Disponible: http://www.virtualeduca.org. Palacio. [Consulta: 2006, Junio 11]

GOLEMAN, D. (2004), **La inteligencia emocional en la empresa**, Vergara, Prov. de Buenos Aires.

GUTIÉRREZ, J. J. (1993). **Una aproximación comprensiva a la relación entre creatividad y aprendizaje a partir de un taller creativo con estudiantes universitarios de psicología**. Tesis para optar al Titulo de Psicólogo.Temuco: Universidad de La Frontera.

GUTIÉRREZ, J.J. (2003). **Modelo Inncrea: Ciclo Vivencial de Aprendizaje Creativo.**Documento Interno no Publicado. Temuco: Innovación & Creatividad Consultores

GORZ ANDRÉ. **Sociedad de la Información/Sociedad del Conocimiento**-*L'immatériel*. - Galilée, 2004. - citación p. 13. [Documento en Línea]. Disponible: http:www.vecam.org/articIe518.htmI[Consulta: 2006, Julio 11]

HERNÁNDEZ, R. Y OTROS (1991). **Metodología de la Investigación.** México: Editorial Mc Graw-Hill.

HURTADO, J. (1998). **Metodología de la Investigación Holística**. Caracas: Fundación para el Desarrollo de la Ciencia y la Tecnología Honey, P.; Mumford, A. (1986): "The Manual of LearningStyles". Maidenhead, Berkshire. P. Honey, ArdinglyHouse.

ISACA (2002). Disponible en http://www.isaca.org página vigente al 16 de abril de 2004.

INTOSAI. Estándares de Auditoria

ISO. 27000.es. Información y recursos para la implantación de Sistemas de Gestión de Seguridad de la Información certificables en ISO 27001. Disponible: http://www.iso27000.es/

KAPLÚN M. (1995). **Los Materiales de autoaprendizaje. Marco para su elaboración**. Santiago, Chile: UNESCO; p.55

KOLB, D.A (1984).**Experientiallearning: experience as thesource of learning and development.**prentice hall, englewoodcliffs, n.j., 1984. 24

LARRAIN, A. Y OTRO (2004). **Formación Universitaria por Competencias**[Documento en Línea]. Disponible: http: www.uis.edu.co/portal/doc_ interes/documentos/. [Consulta: 2006, Septiembre 11]

LAUDON K, Y LAUDON J. (2004). **Sistemas de Información Gerencial. Administración de la Empresa Digital.** México. 8va. Edición. Editorial Pearson Educación.

LE BOTERF, G. (1993): **Cómo gestionar la calidad de la formación**, Barcelona, Gestión 2000.

LEY ORGÁNICA DE EDUCACIÓN (1980). Gaceta Oficial de la República de Venezuela, 2.635 (Extraordinario), Julio 28, 1980.

LEY DE UNIVERSIDADES (1970). Gaceta Oficial de la República de Venezuela, 1.429 (Extraordinario). Septiembre 8, 1970.

LEWIN, K. (1946). **Actionresearch and minorityproblems.** Journal of Social Issues**,** *2* (4), pp. 34-46.

MARTÍNEZ M., M (2006). **La Nueva Ciencia Su Desafío, Lógica y Método.** México, Argentina, España, Colombia, Puerto Rico, Venezuela: Editorial Trillas.

MENA, I. (1992). **Reflexiones imprescindibles para la incorporación de la creatividad en el sistema educacional chileno**. En Lopez, R. & Mena, I. (Ed), Las ovejas y el infinito (pp. 167-168). Santiago: *CPU.*

MESTRA D. L., OLIVO J. Y ROMERO I. (2005). **Estrategias didácticas para el desarrollo de competencias laborales específicas en la asignatura ingeniería Web del programa de ingeniería de sistemas de la corporación educativa mayor del desarrollo Simón Bolívar.** Barranquilla Corporación Educativa Mayor del Desarrollo Simón Bolívar Instituto de Postgrados Especialización en Pedagogía de la Ciencia.

MUÑOZ, J. F., QUINTERO, J. Y MUNÉVAR, R. A. (2002). **Experiencias en investigación acción-reflexión con educadores en proceso de formación**. Revista Electrónica del Investigación Educativa, *4* (1).

Consultado el día 15 de Septiembre de 2005, en: http://redie.uabc.mx/vol4no1/contenido-munevar.html

ORELLANA, N.; BO, R.; BELLOCH, C. Y ALIAGA, F. **"Estilos de aprendizaje y utilización de las TIC en la enseñanza superior".** Unidad de Tecnología Educativa. Dpto. MIDE. Universidad de Valencia.http://www.virtualeduca.org/virtual/actas2002/actas02/117.pdf

PEÑARANDA Q., HÉCTOR R. (2001). **Iuscibernética:Interrelación entre el Derecho y la Informática.** Fondo Editorial para el Desarrollo de la Educación Superior. (FEDES). Caracas Venezuela.

PERNALETE, OLID (2005). **El Desempeño Docente en el aula del Profesional de Informática bajo el Enfoque de Calidad.** Universidad Pedagógica Experimental Libertador. Instituto Pedagógico Barquisimeto "Luis Beltrán Prieto Figueroa.

PIATTINI, M. Y DEL PESO E., (2001). **Auditoria Informática. Un Enfoque Práctico**. 2da. Edición Ampliada y Revisada. Alfa Omega Grupo Editor, S.S. de C.V. México

PINTO CUETO, LUISA, (1999). **Currículo por Competencias: Necesidad de una Nueva Escuela.** Tarea Nº 43 (marzo 1999), 10-17.[Documento en Línea]. Disponible: http: www.uis.edu.co/portal/doc_interes/documentos/. [Consulta: 2006, Septiembre 28]

POSADA A., RODOLFO (2004). **Formación Superior Basada en Competencias, Interdisciplinariedad y Trabajo Autónomo del Estudiante**, Revista Iberoamericana de Educación (ISSN: 1681-5653), Facultad de Educación, Universidad del Atlántico, Colombia

RODRÍGUEZ I, LILIANA. (2005).**Herramienta para Medición de las Competencias Genéricas de los Futuros Ingenieros respecto de las Relaciones Interpersonales**. Revista de Informática Educativa y Medios Audiovisuales Vol. 2(6), págs. 7-16. 2005

RUIZ L. Y CASTAÑEDA A. (2004). **La introducción de foros electrónicos asincrónicos para el perfeccionamiento de la función docente de los profesores desde concepciones de la gestión de la innovación tecnológica.** Cuba, Universidad de las Ciencias Informáticas.

RUIZ, L. (1992). **Gerencia en el Aula**. Nirgua: Editorial INSTIVOC.

REPUBLICA BOLIVARIANA DE VENEZUELA, 2001. LEY ESPECIAL CONTRA DELITOS INFORMATICOS.

REPUBLICA BOLIVARIANA DE VENEZUELA. 2001. LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRONICAS

REPUBLICA BOLIVARIANA DE VENEZUELA. 2001. LEY ORGANICA DE CIENCIA, TECNOLOGIA E INNOVACION

RIVAS, GONZALO ALONSO. 1988. Auditoría Informática. 198 páginas. Ediciones Díaz de Santos. ISBN 84-87189-13.

STONER, FREEDMAN Y GILBERTH: Administration . Ed. Prentice Hall . Edición 1996.

STENHOUSE, L. (1998). **La investigación y el desarrollo del currículum**(4ª. Ed.). Madrid: Morata.

TAYLOR, S. J. Y BOGDAN, R. (1996).**Introducción a los métodos cualitativos de investigación.** Barcelona: Paidós.

TEPPA, S. (1999) **Relación entre las Estrategias Didácticas Constructivistas, Creatividad y Aprendizaje en Biología Celular.** Trabajo de ascenso presentado como requisito para ascender a la categoría de asistente. Universidad Pedagógica Experimental Libertador. Barquisimeto (Venezuela).

THOMAS, J. (2000). A review of researchonproject-basedlearning [Online]. Available:[Documento en Línea]. Disponible: http://www3.autodesk.com/adsk/files/327085_PBL_Research_Paper.pdf[Consulta: 2006, Junio 25]

TUNING EDUCATIONAL STRUCTURES IN EUROPE. INFORME FINAL, FASE UNO. Editado por González, Julia &Wagenaar, Robert. U. de Deusto & U. de Groningen, 2003.

UNDA, O. (2004). **ModuloInstruccional Introducción a la Computación.** Barquisimeto Universidad Centrooccidental “Lisandro Alvarado”.

UNESCO, “Buildingknowledgesocieties: somepreliminarypoints of reflexion”, [Documento en Línea]. Disponible: http://unesdoc.unesco.org/images/0012/001256/125647e.pdf. [Consulta: 2006, Noviembre 29]

UNESCO, L’UNESCO promeut les ‘sociétés du savoir’ pourmaximiserl’impact des technologies de la communication, 03-10-2003 [Documento en Línea]. Disponible: http://portal.unesco.org/ci/fr/ev.phpURLID=13170&URL_DO=DO TOPIC&URL_SECTION=201.html. [Consulta: 2006, Noviembre 29]

VALDÉS R., MARÍA C., (2006). **Las Competencias Pedagógicas en los creativos Entornos Virtuales de Aprendizajes Universitarios**. Revista Tecnología de Información y Comunicaciones. [Documento en Línea].

Disponible: http: www.gobernabilidad.cl/modules.php[Consulta: 2006, Noviembre 15]