UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

CREACIÓN DE SOFTWARE COMO HERRAMIENTA PARA LA AUDITORÍA EN INFORMÁTICA, CON MODALIDAD WORKGROUP

TESIS

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN INFORMÁTICA

PRESENTAN:
MAJLÁ ZORAIDA ÁLVAREZ FLORES
GUSTAVO ALONSO JUÁREZ GONZÁLEZ

ASESOR: L.C. CARLOS PINEDA MUÑOZ

CUAUTITLÁN IZCALLI, EDO. DE MEX. **2011**

AGRADECIMIENTOS

MAJLA

Agradezco a mis padres Jorge y Juanita por todo el apoyo que recibí a lo largo de mi carrera. Así como a mis hermanos que siempre han estado conmigo.

A mi esposo Gabriel porque fue una parte muy importante en toda mi carrera así como mi bastón para no caer cuando se tornaba difícil. **TE AMO**.

A mis hijos Aisha y Zaid por ser mi motor para seguir adelante y ver que se puede hacer muchas cosas si uno se lo propone.

A mis maestros y compañeros por ser un gran ejemplo y por ser grandes amigos. Gracias por dejarme aprender día a día de ustedes.

A la UNAM por darme la oportunidad de estudiar en esta gran casa de estudios.

Y a Dios por dejarme terminar mi carrera con todas las bendiciones que me diario.

GUSTAVO

A mis padres, a mis hermanos y en general a toda mi familia les agradezco todo su apoyo y sacrificios para conmigo a lo largo de mi vida.

A la UNAM por la oportunidad de poder seguir superándome en todos aspectos, con todo el conocimiento otorgado.

Al Profesor Carlos Pineda Muñoz nuestro asesor y a Majlá compañera, amiga y coautora, por confiar en mi para la realización de esta Tesis juntos, por compartirme sus conocimientos y experiencias, con las mejores intenciones.

Al Ángel que tanto apoyo y aguante me dio para superar retos y poder culminar este trabajo, así como a mis profesores, a mis compañeros y amigos de ayer, hoy y siempre por todo el apoyo y trabajo compartidos.

Índice

CAPÍTULO 1 – Introducción ---------- 7
1.1 – Objetivos ---------- 9
CAPÍTULO 2 – Antecedentes y evolución de la Auditoría ---------- 10
2.1 - ¿Qué es la Auditoría? ---------- 11
2.2 – Nacimiento de la Auditoría ---------- 11
2.3 – Evolución de la Auditoría ---------- 12
2.4 – Tipos de Auditoría y sus tareas principales ---------- 13
2.4.1 – Auditoría con Informática ---------- 14
2.5 – Surgimiento de la Auditoría en Informática ---------- 15
2.6 – Tipos de Auditoría en Informática ---------- 17
- Auditoría de la Ofimática ----------17
- Auditoría de desarrollo ---------- 20
- Auditoría del mantenimiento ---------- 25
- Auditoría de la Dirección ---------- 26
- Auditoría de la Explotación ---------- 29
- Auditoría de Bases de Datos ---------- 31
- Auditoría de Sistemas ---------- 34
- Auditoría de la Calidad ---------- 36
- Auditoría de la Seguridad ---------- 38
- Auditoría de Redes ---------- 40
- Auditoría de Aplicaciones ---------- 42
2.7 – Ética del Auditor en Informática ---------- 43
CAPÍTULO 3 – Metodologías para el desarrollo de Auditoría en Informática --- 46

3.1 - Metodología para el desarrollo de una Auditoría en Informática de Mario Piattini ----- 47
3.2 – Metodología para el desarrollo de una Auditoría en Informática
de José Antonio Echenique ---------- 50
CAPÍTULO 4 – Metodología propuesta ---------- 54
4.1 – Metodología propuesta de tesis ---------- 54
CAPÍTULO 5 – Conceptos de Ingeniería de Software ---------- 57
5.1 - ¿Qué es la Ingeniería de Software? ---------- 58
5.2 – Características de los productos de Ingeniería de Software ---------- 59
5.3 – Modelos que maneja la Ingeniería de Software ---------- 60
CAPÍTULO 6 – Tecnologías Web y Software para trabajo en grupo WorkGroup ---------- 66
6.1 – Tecnologías Web, características ---------- 67
6.2 – Lenguajes de marcado HTML, XML, XHTML ---------- 68
6.3 – Lenguaje Script PHP ---------- 72
6.4 – SGBD, Administrador de Bases de Datos MySQL ---------- 74
6.5 – Software para trabajo en grupo WorkGroup, características ---------- 75
CAPÍTULO 7 – Análisis, diseño y programación del sistema propuesto ---------- 77
7.1 – Análisis del sistema ---------- 78
7.2 – Diseño del sistema ---------- 79
7.3 – Programación del sistema ---------- 80
COCLUSIONES ---------- 86
BIBLIOGRAFÍA ---------- 88
ANEXO, DIAGRAMAS DE FLUJO ---------- 89

CAPÍTULO 1

Introducción

1 Introducción

La Auditoría por definición, se entiendo como la actividad de proporcionar una opinión profesional, que surge de someter un objeto al análisis de sus cualidades y su realidad en el entorno donde se encuentra, basándose en métodos establecidos que ayudan a descubrir si las cualidades de dicho objeto son cumplidas según las condiciones prescritas.

Para esto, desde el nacimiento de la Auditoría, hasta la evolución que ha tenido hoy en día en sus diversas clases, ésta ha sido adaptada en diversas disciplinas, desde la Administración, Contabilidad y Finanzas, hasta las áreas de trabajos específicos en sistemas de información, redes y comunicaciones.

La Informática se puede definir desde diversos ángulos, llegando a una misma esencia y concepción, siendo ésta, una ciencia aplicada, dedicada al estudio del tratamiento de la información de forma automática, valiéndose del uso de equipos y sistemas de cómputo para su procesamiento, desde la entrada de los datos, su proceso y la salida de la información, con el objeto de ayudar a la toma de decisiones.

La Informática se ha convertido en una herramienta poderosa en diversos ámbitos, desde una pequeña aplicación para hacer un escrito con formato sencillo o complejo, hasta la creación de sistemas que controlan nuestra vida diaria, en electrodomésticos, autos, telefonía y diversión, pasando por sistemas para la manipulación de grandes maquinarias de Ingeniería y hasta el control del tráfico de una ciudad desde una pequeña sala de computo.

Ha pasado por varias etapas evolutivas, desde las grandes Mainframes compuestas por grandes transistores, resistencias y bulbos, hasta llegar a tener un chip procesador del tamaño de una uña que manipula grandes volúmenes de información. Pero ahí no para su evolución, a cada día y cada hora se están perfeccionando de múltiples formas con distintas herramientas tanto específicas como de uso general todos esos sistemas, aplicaciones, equipos y métodos de programación que contempla la Informática.

Recordando que aquella persona u organización que posee la información tiene grandes ventajas por sobre sus similares, pero el que la sabe manejar tiene más oportunidades de alcanzar el éxito. Además del hecho de que siempre se debe de tener en buen estado las herramientas y métodos con que se

manipula la información, es que se ha decidido realizar esta tesis, con el título de "Creación de software como herramienta para la Auditoría en Informática, con modalidad WorkGroup". Esto con el fin de proporcionar una herramienta, que facilite y simplifique el trabajo a realizar en una Auditoría de las áreas que contemplan los sistemas de información, así como los equipos y métodos para su buen manejo.

Tomando información de diversas fuentes, basándose en diversos puntos de vista y teorías de distintos autores, es que se llegó a la determinación del diseño y forma que tendrá el software que a continuación se presenta. Abarcando desde principios básicos, de los temas principales de Auditoría e Informática, las posibles herramientas para el diseño, creación y manejo de sistemas de información y los conocimientos adquiridos a lo largo de los estudios realizados en la Licenciatura en Informática, se podrán cumplir los objetivos fijados para este trabajo de tesis. Esperando sean funcionales tanto para los autores de dicho trabajo, como para la comunidad entera de la Universidad Nacional Autónoma de México y al país.

1.1 Objetivos

El presente trabajo de tesis presenta los siguientes objetivos, con el fin de demostrar la aplicación y uso de herramientas que faciliten el proceso de una Auditoría en Informática de cualquier organización que cuente con uno o más equipos de cómputo, y con lo que a estos se relacionan, desde el compartir recursos vía Red, hasta los procesos y comunicaciones que ayuden a la toma de decisiones optima y oportuna.

Dichos objetivos son:

- Desarrollar Software con tecnologías Web, que permita el trabajo en grupo para generar información técnica en forma colaborativa.
- Instrumentar una herramienta de apoyo a la realización de Auditorías en Informática.

Conforme avanza el desarrollo de este trabajo, se mostrara la factibilidad de dichos objetivos y su aplicación en el desarrollo de la Auditoría en Informática.

CAPÍTULO 2

Antecedentes y evolución de la Auditoría

2.1 ¿Que es la Auditoría?

El origen de la palabra auditoría proviene del latín "auditorius", de aquí resulta "auditor", que significa, el que tiene la virtud de oír. El diccionario lo define como "revisor de cuentas colegiado".

Toda y cualquier Auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Este concepto se puede descomponer en los siguientes elementos fundamentales:

- Concepto: Es solo una opinión del estado actual.
- Condición: Tiene que ser hecha de forma profesional.
- Justificación: Tiene que tener sustento en determinados procedimientos.
- Objeto: Una determinada información obtenida en un cierto soporte.
- Finalidad: Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

Un distintivo principal de las sociedades en las que vivimos es, la enorme cantidad de información que arrojan día con día. El volumen de información que arroja una empresa, no solo está ligada a sus empleados, sino también a otros, como los usuarios, clientes, etc.

Para que toda esta información nos dé respuestas correctas, es necesario que esté complementada con algunas garantías que nos haga creer en ella. Se requiere de un Auditor, que nos garantice el poder creer en la información.

El Auditor debe de indicar un informe, pidiendo a la empresa se ésta está de acuerdo de cómo se ha realizado este informe.

2.2 Nacimiento de la Auditoría.

La Auditoría ha existido desde siempre, solo que tal y como la conocemos y podemos entender, se comenzó a gestar desde la Revolución Industrial.

Al principio de la Revolución Industrial, la misión del Auditor era la de encontrar algún fraude cometido en los negocios, dichos negocios eran pequeños y no existían las transacciones grandes.

Con el surgimiento de la S. A. (Sociedad Anónima), se ve la necesidad de contratar a un experto que descubriera el ¿porque? de los fraudes y las quiebras importantes, un experto que, controle a los contables, con la confianza de todos los socios de la empresa, ya habiendo distinguido la propiedad de la gerencia. Todo esto, sujeto a al secreto profesional.

Es en Edimburgo Escocia, donde se da el nacimiento de la primera sociedad de Auditores y la primera sociedad oficial nace en 1880 en Inglaterra. A su vez, se da la necesidad de adecuarse a todos esos cambios que se daban con el crecimiento de los negocios y de las cuentas, con la ampliación de las empresas y la descentralización de éstas.

2.3 Evolución de la Auditoría

Cuando las empresas comienzan a crecer, se da una separación entre el capital y el negocio, surgiendo la Administración. Aquí el trabajo del Auditor, dentro de las mismas actividades de un inicio, era el de certificar, y verificar que la información que los administradores le daban en las cuentas de resultados fuera veraz.

Tiempo después, aparecen nuevas tecnologías y modelos de Auditorías, así como computadoras. Las transacciones crecen en volúmenes cada vez más grandes a lo largo del año. El Auditor ya no solo tiene que revisar las cuentas, sino que también tiene que revisar el sistema de control interno de la empresa.

El término Auditoría o Auditores ya se escuchaba en las sociedades Romana y Egipcia antiguas. En el momento en que se tenían que pagar las cuentas de forma verbal a los Auditores, quienes eran los que oían.

Dentro de la Evolución se dan algunos cambios destacables, como por ejemplo; hablando de su objetivo paso de controlar los posibles situaciones irregulares a emitir la opinión acerca de la veracidad en lo que reflejan las cuentas anuales con la imagen fiel de la empresa. En cuanto a lo que consiste, se consideraba un examen exhaustivo y caro y después paso a ser una técnica de muestreo que no consideraba todos los datos (resultado incompleto o no muy confiable).

Hablando del reporte o documento que se emite, pasó de ser una certificación de la situación a una opinión profesional por la calidad, la confiabilidad y la certeza de la que trata. El papel del Auditor no se puede dejar de lado, ya que es en el Auditor en quien se confía la opinión de la situación, antes el Auditor era quien asumía la exactitud de todas las cuentas y ha cambiado por asumir que las cuentas reflejan la imagen fiel, como conjunto.

Hoy en día, la Auditoría ha tomado un papel tan cotidiano y obligatorio en las diversas empresas y organizaciones debido al gran crecimiento en los negocios y transacciones al rededor del mundo, llegando a verle como una herramienta elemental para preservar el control, ya no solo de las cuentas, sino de hasta sistemas y seguridad como es el caso de la Auditoría Informática.

2.4 Tipos de Auditoría y sus tareas principales.

Para esto, se puede ejemplificar de la siguiente forma:

Financiera: en la cual, el contenido es solo una opinión de las cuentas anuales y de la veracidad de los estado financieros, así como, la preparación de los informes en aspectos contables, que presentan la realidad en la organización o área auditada.

Gestión u operacional: solo es una opinión dirigida a la dirección de la organización, en la cual se refleja la eficacia, eficiencia y economicidad, en los métodos y procedimientos que rigen un proceso de la misma organización o empresa.

Fiscal: esta solo se dedica a observar el cumplimiento de las leyes fiscales, sus procedimientos y resultados.

Temáticas: son aquellas que se realizan con el fin de examinar en uno y cuatro temas particulares, abarcando con total profundidad los aspectos relacionados a estos temas, esto para evaluar si se cumplen las regulaciones establecidas en el área a auditar.

Recurrente: aquí se examinan algunas medidas surgidas de Auditorías anteriores calificadas de manera negativa, enfocadas a los demás tipos de Auditorías.

Especiales: enfocadas a la verificación de asuntos y temas específicos. Ya sea de, alguna parte de la operación financiera o administrativa, de hechos o situaciones especiales y todos tienen que responder a una necesidad específica.

Informática: se encarga de recoger, agrupar y evaluar las evidencias necesarias para determinar si un sistema salvaguarda los activos, mantiene la integridad de los datos y hace uso eficiente de los recursos de la organización.

2.4.1 Auditoría con Informática.

En esta parte, se puede tomar en cuenta desde el uso de una PC con unas cuantas aplicaciones básicas de contabilidad, una hoja de cálculo y un procesador de textos hasta un sistema más complejo e integrado por bases de datos en modo cliente - servidor, y comunicado con otros sistemas con los que sé interactúa. Es evidente que las tres Normas para la ejecución de la Auditoría adquieren una complejidad y magnitud diferente. Tanto más está desarrollado el sistema, más problemas resultan en el enfoque del Auditor. Los procedimientos de Auditoría dicen que, "el auditor debe valerse en la ejecución de su trabajo, de medios como la inspección, observación, averiguación, confirmación, cálculo y análisis". De estos, al menos cuatro se pueden hacer de forma más eficiente con medios informáticos:

- En la parte de la inspección se puede entender como la comparación de datos en dos cuentas, archivos o conciliaciones distintas.
- En él cálculo se contemplan, provisiones, gastos, amortizaciones, impuestos, etc.
- El análisis se da en los datos y/o regresiones que cumplan determinadas condiciones.
- La confirmación es el estadístico, la selección y emisión de muestras, el cumplimiento, y otros aspectos que dejen en claro el resultado del trabajo final de la Auditoría.

Esto nos refleja que las posibilidades del Auditor se maximizan al momento de utilizar medios electrónicos e informáticos con respecto a trabajos manuales sobre listados, registros y reportes en papel, además del incremento evidente en, la velocidad, la eficiencia y la seguridad.

Para lograr todo lo anterior, el Auditor podrá valerse de las diferentes herramientas informáticas que tiene a su alcance y que se podrían catalogar de la siguiente forma:

De tipo "General", donde la planificación de la Auditoría se da con el tratamiento de textos, el flowcharting y las utilidades y la ejecución de la Auditoría se da en tratamiento de textos y hojas de cálculo.

De "Acceso directo", con la ejecución de la Auditoría en ``ACL (Audit Command Language)".

De tipo ``Específico", aquí la planificación de la Auditoría se da con los generadores de papeles de trabajo y la Administración y la ejecución se da en simulación paralela y revisión analítica.

Y las de tipo ``Especializado", con la planificación y la ejecución de la Auditoria echas con integradores, sistemas expertos y Test check.

2.5 Surgimiento de la Auditoría en Informática

La Auditoría en Informática es el proceso dedicado a recolectar evidencias y datos, agruparlos y hacer una evaluación de los mismos, con el fin de determinar si un sistema que ya está informatizado salvaguarda en primera instancia los activos, mantiene la integridad de los datos, permiten de forma eficaz los fines de la organización y utiliza eficientemente todos los recursos del mismo sistema.

¿Cómo surge la Auditoría en Informática?

Debido a la especialización de las actividades computacionales, así como por el gran avance que han tenido los sistemas en los últimos años, ha surgido una nueva necesidad de evaluación para los auditores. Estos requieren de especialización cada vez más profunda en sistemas computacionales para dedicarse a este tipo de auditoría.

La Informática está muy mezclada a la gestión integral de la empresa, y por ello los procedimientos, normas y estándares informáticos están sometidos a los generales de la empresa. Por esto los sistemas informáticos forman parte de la gestión de la empresa, pero no quiere decir que la informática gestione

propiamente a la empresa, sino que, hace uso de ella para la toma de decisiones y no decide por sí misma. Debido a la importancia que tienen los sistemas computacionales en el funcionamiento de la empresa actualmente existe la Auditoría en Informática.

``El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa".[1]

El nacimiento de la metodología en el mundo de la Auditoría y el control interno Informático se puede apreciar en los primeros años de la década de los 80, conociéndose entonces como Auditoría de sistemas. Esta utiliza la metodología de las disciplinas como la seguridad de los sistemas de información que es la que trata los riesgos informáticos. Es ahí donde la auditoría se involucra en los procesos de protección y preservación de toda información y de sus medios de proceso.

La definición del autor Ron Weber dice:

“Es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas computarizados, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficient".[2]

De este modo la Auditoría en Informática sustenta y confirma la consecución de los objetivos de la Auditoría:

- Objetivos de protección e integridad de datos.
- Objetivos de gestión que abarcan, no solo los de protección de activos, sino también los de eficacia y eficiencia.

El Auditor es el encargado de evaluar y comprobar en determinados momentos los controles y

1 Auditoría en Informática, Piattini, Mario.
2 Auditing Conceptual Foundations and Practice, Weber, Ron.

procedimientos informativos más complejos , con el desarrollo y aplicación de técnicas mecanizadas de Auditoría contemplando el uso de software.

En muchos casos no es posible verificar manualmente los procedimientos informatizados que administran los datos, por lo que se deberá emplear algún software de auditoría y otras técnicas asistidas por computadora.

``El Auditor es el responsable de precisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada".[3]

Se pueden establecer tres grupos de funciones a realizar por un Auditor Informático:

- Puede participar en revisiones durante y después del diseño, en la realización, implementación y explotación de las aplicaciones informativas, así como en fases de cambios importantes.
- Revisar y juzgar los controles de los sistemas informativos para verificar que se hayan cubierto las ordenes de la Dirección, requisitos legales, protección de confidencialidad y cobertura de errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

2.6 Tipos de Auditoría en Informática

AUDITORÍA DE LA OFIMÁTICA

La Ofimática se refiere al sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina. Este concepto nace a comienzos de la década de los años 90, y sus primeras aplicaciones se desarrollan sobre las computadoras centrales de las organizaciones. A pesar de que se ha considerado a las oficinas como pioneras en el uso de herramientas informáticas para el desempeño de sus actividades, es en ese tiempo que se ha producido un espectacular crecimiento en la demanda de los sistemas de ofimática que hoy sigue creciendo.

3 Auditoría en Informática, Piattini, Mario.

Algunos ejemplos de esto son: las aplicaciones de gestión de tareas, procesadores de texto y hojas de cálculo, herramientas de gestión de documentos y bases de datos, control de expedientes, agendas, sistemas de trabajo en grupo como correos electrónico o el control de flujos de trabajo, etc.

Este desarrollo de sistemas ofimáticos ha mantenido dos modelos fundamentales: el escritorio virtual y el trabajo cooperativo (CSCW, Computed Supported Cooperative Work).

Un ejemplo de escritorio virtual es un escritorio virtual visto en la pantalla de la computadora, que toma el lugar de la mesa de trabajo tradicional. En dicho escritorio virtual se encuentran las herramientas necesarias para desarrollar las actividades de oficina. La interfaz virtual debe ser familiar al usuario y de fácil aprendizaje para darle el uso adecuado. Todas las herramientas y aplicaciones deben de ser compatibles e integrarse perfectamente entre sí.
El CSCW podría considerarse una extensión de la integración de aplicaciones. Es la multiplicidad de actividades coordinadas, desarrolladas por un conjunto de participantes y soportadas por un sistema informático. El entorno ofimático además de permitir el trabajo individual debe permitir el intercambio de información necesaria de los diversos procesos de la organización, así como interacciones con otras organizaciones.

En el área de la ofimática se tienen dos características distintivas; la distribución de las aplicaciones por los diferentes departamentos de la organización en vez de estar en una ubicación central; y el traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios finales no dedicados a la informática.

A consecuencia de dichas características, se han generado problemáticas referentes al entorno como lo son: falla en adquisiciones; desarrollos ineficientes e ineficaces; errores en los usuarios al manejar la seguridad de la información; uso de copias ilegales en aplicaciones; etc. Por lo cual se debe contemplar una serie de controles seleccionados para poder ser aplicados a cualquier organización, pero con la libertad de agregar más controles adicionales si la organización lo requiere o en algunos casos los controles propuestos no podrán ser los necesarios a la organización.

Estos controles se presentan agrupados con criterios relacionados con aspectos de economía, eficacia y

eficiencia, seguridad y aspectos legales que son base para la labor del Auditor.

En lo que respecta a los controles de la ofimática en la economía, eficacia y eficiencia se deben contemplar aspectos de control como:

- Determinar sí el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.
- Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.
- Determinar y evaluar la política de mantenimiento definida en la organización.
- Evaluar la calidad de las aplicaciones del entorno ofimático desarrollada por personal de la propia organización.
- Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.
- Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente.
- Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

En los controles de la seguridad ofimática se contemplan los siguientes:

- Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.
- Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.
- Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer perdidas de integridad de la información y aplicaciones.
- Determinar el grado de exposición ante la posibilidad de intrusión de virus.

En el aspecto de la legalidad de la ofimática se toman en cuenta los siguientes controles para tener un mejor apego a la ley:

- Se debe determinar si en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto en la Ley Orgánica 51/1999, de protección de datos de carácter

personal (LOPD).

- Determinar si en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto en el Real Decreto Legislativo 1/1996, sobre la propiedad intelectual.

En gran parte de las aplicaciones de auditoría en el aspecto de ofimática no hay mucha diferencia de las actuaciones necesarias para auditar sistemas centralizados, ya que en todos los casos la experiencia del Auditor es la que importa más para la selección de los controles y la adecuación de los mismos al sistema a auditar, tomando en cuenta la evolución que tienen día a día las herramientas de ofimática, lo cual requerirá de conocimientos específicos y actualización en técnicas novedosas.

AUDITORÍA DE DESARROLLO

Teniendo en cuenta que cada organización puede fraccionarse en distintos departamentos o áreas, es necesario que los mecanismos de control están y se respeten, para que dichas áreas cumplan adecuadamente su cometido y hagan que la organización funcione correctamente en conjunto. Dentro de estas áreas es común que en la misma área de informática se encuentra la de desarrollo.

Para saber los límites de acerca de la auditoría de desarrollo, se debe entender por desarrollo incluye todo el ciclo de vida del software excepto la explotación, el mantenimiento y la retirada de servicio de las aplicaciones cuando ésta tenga lugar.

La Auditoría de desarrollo tratará de verificar la existencia y aplicación de procedimientos de control adecuados que permitan garantizar que el desarrollo de sistemas de información se ha llevado a cabo según los principios de la Ingeniería de software o determinar las deficiencias existentes.

Existen algunas circunstancias que hacen particularmente importante al área de desarrollo y también su auditoría en comparación a otras áreas del departamento de Informática:

- Los avances en tecnologías de computación han provocado el desafío más importante de la informática sea la mejora de la calidad del software.
- El gasto del software es cada vez mayor al que se hace en hardware.

- A comparación del poco tiempo de la Informática, hace tiempo que surgió la crisis del software, que refleja problemas como el desarrollo y mantenimiento de software que afecta gran número de organizaciones. El área del hardware no ha sido tan afectada.
- Es difícil dar un valor al software como producto, ya que en medida de que se desarrolla su calidad se incrementa su costo, pero se descuida su mantenimiento.
- El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual denota la inexistencia o mal funcionamiento de los controles en este proceso.

Para tratar esta Auditoría se deben delimitar las funciones que son responsabilidad del área. Contemplando que pueden existir variaciones de una organización a otra, y las funciones que se asignan a esta área de forma tradicional son:

- Planificación del área de Informática y su participación en la elaboración del su plan estratégico.
- Desarrollo de nuevos sistemas contemplando para cada sistema, el análisis, diseño, construcción e implantación, dejando el mantenimiento a otra área.
- Estudio de nuevos lenguajes, técnicas, estándares, metodologías, herramientas entre otros, relacionados con el desarrollo de sistemas, para mantener un nivel de vigencia adecuado a la tecnología al momento.
- Establecimiento de un plan de formación para el personal adscrito al área.
- Establecer normas y controles para las actividades que se realizan en el área y comprobación de su observación.

Ya que se conocen las tareas a realizar, la auditoría de esta área se divide en dos apartados:

- Auditoría de la organización y gestión del área de desarrollo.
- Auditoría de proyectos de desarrollo de sistemas de información.

Auditoría de la organización y gestión del área de desarrollo.

Cada proyecto tiene su identidad y gestión propia, y para que puedan realizarse, se deben apoyar en el personal del área y sus procedimientos establecidos.

Para la importancia de esta auditoría se han considerado 8 objetivos de control (serie A):

- Objetivo de control A1: El área de desarrollo debe tener cometidos asignados dentro del departamento y una organización que le permita el cumplimento de dichos cometidos.
- Objetivo de control A2: El personal de esta área deberá tener la formación adecuada y la motivación para realizar su trabajo.
- Objetivo de control A3: En caso de existir un plan de sistemas, todos los proyectos que se realicen se basaran en el plan y se mantendrá actualizado.
- Objetivo de control A4: La propuesta y aprobación de nuevos proyectos debe realizarse de forma reglada.
- Objetivo de control A5: La asignación de recursos a los proyectos debe hacerse de forma reglada.
- Objetivo de control A6: El desarrollo de sistemas de información debe hacerse aplicando principios de ingeniería de software ampliamente aceptados.
- Objetivo de control A7: Deberá existir un procedimiento para las relaciones con el exterior del departamento.
- Objetivo de control A8: La organización del área debe estar adaptada a las necesidades en todo momento.

Auditoría de proyectos de desarrollo de S. I.

Como lo menciona el apartado anterior, cada proyecto tiene su identidad propia, así como también, tienen objetivos marcados que podrán afectar determinadas unidades de la organización. Por ello, debe tener un responsable y ser gestionado con técnicas que permitan alcanzar sus objetivos, tomando en cuenta los recursos disponibles y restricciones temporales del mismo. Aquí se requiere de la colaboración de todas las partes de la organización a las que afecte el sistema.

La auditoría de cada proyecto varía con la complejidad y los riesgos del mismo, lo cual, orilla a que la pericia y experiencia del Auditor sean las que controlen las actividades en función de los parámetros mencionados.

Este apartado define objetivos y técnicas de control generales y aplicables a cualquier proyecto, dando libertad al Auditor de decidir los más importantes para las características del proyecto y la fase a auditar.

Los controles propuestos para este apartado, toman en cuenta las fases de la elaboración de sistemas de información como lo son; análisis, diseño, construcción e implantación, que son ampliamente aceptadas por la Ingeniería de software para el desarrollo. Además una subdivisión que contempla técnicas de control referentes a la aprobación, planificación y gestión del proyecto.

- Aprobación, planificación y gestión del proyecto. Aquí se contemplan dos objetivos de control (serie B).

- Objetivo de control B1: El proyecto debe estar definido, planificado y aprobado formalmente.
- Objetivo de control B2: El proyecto se debe manejar de la mejor forma para conseguir los mejores resultados, contemplando restricciones de tiempo y recursos. Además de que los criterios establecidos deberán concordar con los objetivos de las áreas afectadas.

- Auditoría de la fase de análisis. Aquí se obtienen especificaciones que describen las necesidades de información a ser cubiertas por el nuevo sistema de manera independiente al entorno técnico. Esta fase se divide en dos módulos:

- Análisis de requisitos del sistema (ARS): aquí se identifican los requisitos del nuevo sistema distinguiendo importancia y prioridad.

- Objetivo de control C1: Tanto los usuarios como responsables de las unidades afectadas por el nuevo sistema, deben establecer los requisitos del mismo.
- Objetivo de control C2: En el proyecto se utilizara la alternativa más favorable para que el sistema cumpla los requisitos establecidos.

- Especificación funcional del sistema (EFS): Una vez establecidos los puntos anteriores se elaborará

una especificación funcional detallada del sistema que sea coherente con lo que se espera del sistema mismo. Los usuarios y responsables deben ser la fuente principal de información para las entrevistas para el análisis de requisitos del sistema y aquí se considera un único objetivo de control (serie D).

- Objetivo de control D1: Aquí se define la forma en que interactúan el sistema con los distintos usuarios, ya que los mismos usuarios definirán la forma de trabajo con el sistema.

- Auditoría de la fase de diseño. Aquí se elaborará el conjunto de especificaciones físicas del nuevo sistema que servirán de base para su construcción. Hay un único modulo denominado, Diseño Técnico del Sistema (DTS). Donde se diseñara la arquitectura del sistema y el esquema externo de datos.

- Objetivo de control E1: Aquí se define la arquitectura para el sistema, acorde a la especificación funcional y el entorno tecnológico elegido.

- Auditoría de la fase de construcción. En esta fase se programan y prueban los componentes y se ponen en marcha los procedimientos necesarios para que los usuarios puedan trabajar con el sistema, basándose en la fase de diseño y consta de dos módulos.

- Desarrollo de los componentes del sistema (DCS): En este módulo se realizan los distintos componentes, donde se prueban de forma individual e integrada, con el desarrollo de los procedimientos del sistema. Con un único objetivo (serie F).

- Objetivo de control F1: Los componentes deben desarrollarse usando técnicas de programación correctas.

- Desarrollo de los procedimientos de usuario (DPU): Aquí se definen los procedimientos y formación necesarios para el uso adecuado del sistema por los usuarios. Se trata de la instalación, la conversión de datos y la operación / explotación del sistema. Considerando un único objetivo de control (serie G).

- Objetivo de control G1: Una vez terminado el proyecto, se deberá capacitar a los usuarios, y disponerles de todo los medios para hacer uso del sistema.

- Auditoría de la fase de implantación. En esta fase se da la aceptación del sistema por los usuarios.

Además de las actividades necesarias para ponerlo en marcha y solo contempla un solo módulo.

- Pruebas, implantación y aceptación del sistema (PIA): Este módulo ayuda a verificar, que el sistema cumple con todos los requerimientos establecidos. Una vez aprobado se pondrá en marcha.

- Objetivo de control H1: El sistema debe ser aceptado por los usuarios de manera formal antes de su explotación.
- Objetivo de control H2: El sistema sé pondrá en marcha y explotación de manera formal, y estará en mantenimiento solo cuando haya sido aceptado y esté preparado todo el entorno en el que se ejecutará.

"A pesar de ser una de las actividades principales de la Informática, el desarrollo de software no ha conseguido alcanzar de forma general unos parámetros de calidad aceptables".[4]

Todas las actividades dentro del desarrollo de sistemas de información tienen la misma importancia al momento de realizar auditoría, puesto que por mucho que se piensa que la programación es la parte más importante, se ha detectado que los errores cometidos en las actividades iniciales de los proyectos son más costosos que los que se producen al final del desarrollo.

AUDITORÍA DE MANTENIMIENTO

La atención a la Auditoría en Informática que se la había prestado a esta etapa de cualquier sistema de información ha sido poca, donde solo se advertían una pequeña parte de los problemas, y solo se empleaba un mínimo esfuerzo en técnicas de Auditoría para esta etapa.

Se he llegado a conclusiones por medio de investigaciones, que la etapa de mantenimiento consume la mayor parte de los recursos empleados en un proyecto de software y por tanto esta etapa debe ser considerada en los estudios de la Auditoría en Informática. La mantenibilidad es un factor de calidad crítico, que estudia la Auditoría en Informática del Mantenimiento. Este factor muestra las características que hacen un producto de más fácil mantenimiento y más productivo.

4 Auditoría en Informática, Piattini, Mario.

La cantidad de esfuerzo que se dará en la Auditoría del mantenimiento se empieza a medir desde las primeras etapas del desarrollo de software y con frecuencia son olvidados. En las especificaciones del software como en la ingeniería de requisitos se verán los aspectos que determinaran el esfuerzo o no dificultad del mantenimiento del software.

SI la productividad en la etapa de mantenimiento es baja, puede suceder que el equipo humano que desarrolló el sistema se dedique de tiempo completo a su mantenimiento. Provocando que si la organización decide la realización de nuevos productos de software, tendrá que incluir un nuevo equipo para realizarlo. Esto provoca un desaprovechamiento de experiencia adquirida por el equipo anterior que pudiera ser útil en los nuevos proyectos. Y por consecuencia, una labor extra para que el nuevo equipo adquiera los conocimientos sobre los métodos y herramientas de software que utiliza la organización.

AUDITORÍA DE LA DIRECCIÓN

La dirección de informática no debe quedar fuera: es una pieza clave del engranaje. De una manera general, se podrá decir que algunas de las actividades básicas de todo proceso de dirección son:

- Planificar
- Organizar
- Coordinar
- Controlar

Planificar

Se trata de prever la utilización de las tecnologías de la información en la empresa, existen varios tipos de planes informáticos en la empresa, se debe asegurar el alineamiento de los mismos con los objetivos de la propia empresa. Estos planes no son responsabilidad exclusiva de la Dirección informática. Su aprobación final incumbe a otros estamentos de la empresa: Comité de Informática e incluso en último término de la Dirección General. Sin embargo, la Dirección de Informática debe ser el permanente impulsor de una planificación de Sistemas de Información adecuada y a tiempo.

Dentro de esta actividad se contempla el ``Plan Estratégico de Sistemas de Información", el cual es la base de actuación de los Sistemas de Información en la organización. Este asegura el equilibrio entre los mismos sistemas con los objetivos de la misma organización.
Dicha planeación no es exclusiva de la Dirección Informática, ya que la aprobación final incumbe a otras áreas de la organización, incluso podría llegar a ser decisión de la Dirección General. Sin embargo la Dirección de Informática deberá ser siempre la que tome iniciativa en la planificación de Sistemas de Información adecuada y pronta.

Guía de auditoría

El Auditor examinara el proceso de planificación de sistemas de información y evaluar si se cumplen los objetivos para el mismo en aspectos como:

- En el proceso de planificación se presta atención al plan estratégico de la empresa, se contemplan cambios organizativos, entorno legislativo, evolución tecnológica, recursos, organización informática, etc., todo esto contemplado en el Plan Estratégico de Sistemas de Información.
- Las tareas y actividades incluidas en el Plan tienen la correspondiente asignación de recursos para poderse realizar.

Como se mencionó al principio, existen varios tipos de planes informáticos, otros ejemplos habituales de los mismos son:

- Plan operativo anual
- Plan de dirección tecnológica
- Plan de arquitectura de la información
- Plan de recuperación ante desastres

Organizar y coordinar

En el proceso de organización se estructuran los recursos, los flujos de información y los controles que ayudaran a alcanzar los objetivos establecidos en la planificación.

Comité de Informática

Comúnmente se ha reclamado a la informática y los informáticos la falta de comunicación y entendimiento que existe entre el departamento de informática en la organización y el resto de la misma. El comité de informática es el primer lugar de encuentro dentro de la empresa, tanto de los informáticos como de los usuarios. Evitando así acusaciones de favoritismo entre unas áreas y otras.

Se recomienda que dicho comité este integrado por pocas personas y presidio por el director con el grado señor mas alto dentro de la organización, que tiene responsabilidad en última instancia de las tecnologías de información. El Director de Informática debería fungir como secretario de Comité y las grandes áreas usuarias deberían estar representadas al nivel de sus directores más altos, de igual forma, el director de Auditoria Interna debería ser miembro del Comité.

Posición del Departamento de informática en la empresa

El segundo aspecto importante a contemplar en la evaluación del papel de la informática en la organización, es la ubicación del Departamento de informática dentro de la estructura organizativa de la organización. Esta posición debería otorgarle al Departamento autoridad e independencia frente a los demás departamentos usuarios, dándole un nivel alto de jerarquía y teniendo la cantidad de personal suficiente para lograr dicha autoridad.

La imagen tradicional que se tiene de la informatización de las organizaciones es que se maneja ya sea en el departamento financiero o de administración e integrado en estos se encuentra el departamento de informática. En la actualidad es más común ver al departamento de informática dando soporte a más áreas organizacionales, y dependiendo directamente de la Dirección General

En este aspecto el auditor tiene la tarea de revisar el emplazamiento organizativo del Departamento de Informática y evaluar su independencia frente a los departamentos usuarios.

Controlar

En este punto se recuerda la obligación de la Dirección de controlar y efectuar un seguimiento permanente de la distinta actividad del Departamento. Se vigilara el desarrollo de los planes estratégico y operativo y de los proyectos que los desarrollan, la evolución de la cartera de peticiones de usuarios, los costes, la evolución del equipo de cómputo y de otros recursos, como espacio en disco, comunicaciones, disponibilidad de periféricos, etc.

Es recomendable establecer estándares de rendimiento para comparación de las diversas tareas, las cuales, son aplicables a diversos aspectos de la actividad del Departamento: consumo de recursos del equipo, desarrollo, operaciones, etc.

Así mismo, la Dirección de Informática deberá controlar que la realización de sus actividades se lleva a cabo dentro del respeto a la normativa legal aplicable. Haciendo énfasis en la parte de la seguridad e higiene en el trabajo, normativa laboral y sindical, protección de datos personales, propiedad intelectual del software, requisitos definidos en la cobertura de seguros, transmisión de datos por líneas de comunicaciones, así como normativa emitida por órganos reguladores sectoriales.

AUDITORÍA DE LA EXPLOTACIÓN

El nivel de competencia que existe en la actualidad entre las empresas, obliga a tomar decisiones más rápidas y acertadas. Para lograrlo es necesario el funcionamiento adecuado de los sistemas informáticos, implementando nuevas tecnologías con su respectivo mantenimiento.

En este tipo de Auditoría se elabora el esquema de un procedimiento para llevar a cabo las auditorias de explotación de los sistemas de información.

Se puede considerar un Sistema de Información (SI) como un conjunto de componentes que interactúan en pro de que la empresa alcance sus objetivos satisfactoriamente. Los componentes o recursos de un SI son los siguientes:

- Datos: se consideran tanto los datos estructurados como no estructurados, imágenes, sonidos,

etc.

- Aplicaciones: se incluyen las aplicaciones manuales y las informativas.
- Tecnología: El software y el hardware, los sistemas operativos, los sistemas de gestión de bases de datos y los sistemas de red, etc.
- Instalaciones: En donde se ubican y mantienen los sistemas de información.
- Personal: que deberá contar con los conocimientos para planificar, organizar, administrar y gestionar los sistemas de información.

Estos recursos se han de utilizar de tal forma que permitan la eficacia y la eficiencia de la organización, que los datos financieros procesados en los sistemas de información sean los correctos y que la organización cumpla la legislación vigente, además de que dichos sistemas aseguren la confidencialidad de sus datos conforme a lo contemplado en la legislación vigente.
Carta de encargo

Las responsabilidades del trabajo de auditoría deben quedar recogidas en un contrato o carta de encargo antes de comenzar su realización (la Norma General número 12 de ISACA ``Draft Estándar No. 12''). En ese documento debe quedar reflejado de forma clara cuál será el alcance del trabajo del auditor, entre otros aspectos.

Planificación

Según la Norma General número 6 de ISACA las auditorias de los sistemas de información deben planificarse y supervisarse para tener la seguridad de que los objetivos de las mismas se alcanzan y se cumplan las NASIGAA.

En la planificación de la auditoría se consideran tres fases:

- Planificación Estratégica: Es una revisión global que permite conocer la organización, el SI y su control interno.
- Planificación Administrativa: En esta fase pueden surgir problemas de coincidencia en las fechas de trabajo del personal de la empresa auditora con otros clientes. Es por eso que no se debería hacer hasta haber concluido la - Planificación Estratégica. Aquí se asignan los recursos

de personal, tiempo, etc.

- Planificación Técnica: En esta fase se elaborara el plan de trabajo, los métodos, los procedimientos, las herramientas y las técnicas que se utilizaran para alcanzar los objetivos de la auditoria.

Informes

Una vez realizadas las fases anteriores, el auditor está en condiciones de emitir un informe en el cual se expresa su opinión. Son 4 opiniones básicas usadas en reportes de auditoria:

- Favorable: si se concluye que el sistema es satisfactorio.
- Desfavorable: si se considera que el sistema es un desastre.
- Con salvedades: cuando el sistema es válido pero tiene algunos fallos que no lo invalidan
- Denegación de opinión: cuando no se tengan suficientes elementos de juicio para poder opinar.

En el caso de que se detecten debilidades en la auditoria, se deberá comunicar con prontitud al auditado. Y las debilidades se recomienda presentarlas con el siguiente esquema.

- Describir la debilidad.
- Indicar el criterio o instrumento de medida que se utilizó.
- Indicar los efectos que puede tener en el sistema de información.
- Describir la recomendación con la que esa debilidad se podría eliminar.

AUDITORÍA DE BASES DE DATOS

La importancia en el entorno de la auditoria de bases de datos radica en que es el punto de partida para poder realizar la auditoria de las aplicaciones que utilizan esta tecnología.

En la actualidad, el uso más frecuente de Sistemas de Gestión de Bases de Datos (SGBD), y la importancia de los datos como recursos fundamentales de las organizaciones, han aumentado el interés en aspectos de su control interno y auditoría.

Cuando el auditor, encuentra el sistema de información en explotación, deberá estudiar el SGBD y su entorno. Pero existe el gran problema de que el entorno de las bases de datos es más complejo

conforme avanza el tiempo y no puede solo contemplar el propio SGBD.

Sistema de Gestión de Bases de Datos (SGBD)

De entre todos los componentes del SGBD se destacan, el núcleo (kernel), el catálogo, las utilidades de administración de bases de datos, re arranque, copias de respaldo, archivos generados diariamente, etc. así como algunas funciones de auditoria, así como los lenguajes cuarta generación (L4G) que incorpora el propio SGBD. El auditor deberá revisar todas las herramientas que ofrece el SGBD y las políticas y procedimientos que sobre su utilización haya definido el administrador, para valorar su efectividad.

Software de auditoría

Son paquetes que se pueden usar para facilitar la labor del auditor, referente a la extracción de datos de la base, el seguimiento de las transacciones, datos de prueba, etc.

Sistema de monitorización y ajuste (tuning)

Este tipo de sistemas complementan las facilidades ofrecidas por el mismo SGBD, arrojando mayor información para optimizar el sistema, llegando a ser sistemas expertos que proporcionan la estructura óptima de la base de datos.

Sistema Operativo (SO)

Es una pieza clave del entorno, ya que en él se dará el mayor apoyo del SGBD en cuanto a control de memoria, gestión de áreas de almacenamiento, confidencialidad, control de errores, etc.

Monitor de Transacciones

Se puede considerar un elemento más del entorno con responsabilidades de confidencialidad y

rendimiento.

Protocolos y Sistemas Distribuidos

El acceso a las bases de datos por medio de red, es cada vez mayor, pero el riesgo de violación de la confidencialidad también lo es, así como también el riesgo es alto en las bases de datos distribuidas. Cabe mencionar que las bases de datos distribuidas son más baratas de actualizar en cuanto a la transferencia de archivos y procesos por lotes (batch), que hacerlo en línea.

Paquete de seguridad

Se debe tomar en cuenta que para que el paquete de seguridad sea compatible con el SGBD, se considera la centralización de control de accesos, la definición de privilegios, perfiles de usuario, etc.

Diccionarios de datos

Se puede auditar de manera separada los diccionarios de la base de datos, puesto que los primeros son considerados metadatos, pero se corre el riesgo de que un error en el diccionario produzca errores de forma repetitiva en la misma base de datos, siendo más difíciles de detectar, y provocando mayores riesgos financieros.

Herramientas CASE (Computer Aided System/Software Engineering). IPSE (Integrated Project Support Enviroments)

Conforman una herramienta para que el auditor pueda revisar el diseño de la base de datos, comprobar si se ha empleado correctamente la metodología y asegurar un nivel mínimo de calidad.

Lenguajes de Cuarta Generación (L4G) independientes

Además de las herramientas del mismo SGBD, se puede encontrar una amplia variedad de generadores de aplicaciones, formas, informes, etc. que actúan sobre la base de datos y que también son un elemento importante en el entorno del SGBD.

Facilidades de usuario

Debido a las interfaces gráficas cada vez más amigables con el usuario, donde no es necesario saber la sintaxis de los lenguajes, y las herramientas de gestión de bases de datos son más fáciles, el auditor deberá investigar las medidas de seguridad de estas herramientas para proteger incluso al usuario de sus mismo errores.

AUDITORÍA DE SISTEMAS

Los sistemas se definen como el conjunto de elementos que interactúan unos con otros para un fin específico, solo que en ocasiones se superponen unos en otros y es difícil en ocasiones, identificarlos componentes parciales.
Como ejemplo se tiene la Técnica de Sistemas, que podría abarcar el total del proceso informático o simplemente quedar limitado a una porción del mismo proceso.

Se consideran dentro de la Técnica de Sistemas, tres especialidades:

- Sistemas Físicos
- Informática Fundamental
- Informática de Gestión

De lo cual se determina, que el Técnico en Sistemas se especializa desde el Hardware (Sistemas Físicos) hasta el desarrollo de lenguajes formales de programación hasta los Autómatas (Informática fundamental) y el trabajo de aplicaciones (Informática de Gestión).

Antes de explicar la Auditoría de Técnica de Sistemas, se debe definir la tarea a auditar como una actividad informática que requiere un determinado desempeño profesional, para alcanzar los objetivos propuestos.

La Técnica de Sistemas es, la actividad a desempeñar para la instalación y mantenimiento en adecuado orden la infraestructura informática.

La función adecuada de lo antes mencionado está caracterizada por:

- Disponer de todos los elementos necesarios.
- Por parte de los usuarios autorizados.
- En el momento requerido.
- Don el rendimiento adecuado.

Ya que dicha función se encuentra organizada, se asigna una tarea que se descompone en varias actividades a realizar con procedimientos específicos para garantizar su calidad.

La tarea de la administración de los recursos del Sistema de información debe optimizar algunos parámetros establecidos, a su vez, estos parámetros se han de convertir en el objetivo de los procedimientos a realizar. Y estos procedimientos se pueden clasificar de tal forma que sirva para cualquier elemento de infraestructura, como ejemplo se puede tomar el Sistema Operativo. Los procedimientos se clasifican en:

1- Instalación y puesta en servicio. Aquí se consideran todas las actividades para conseguir el funcionamiento adecuado del elemento en cuestión.
2- Mantenimiento y soporte. Se refiere al conjunto de acciones necesarias para la puesta al día del elemento, así como la asistencia de terceros para la consecución de dicha puesta al día, que facilite información necesaria sobre el sistema para su mejor utilización.
3- Requisitos para otros componentes. Es el procedimiento de requerimientos y recomendaciones para el mejor comportamiento de otros componentes del Sistema de Información.
4- Resolución de Incidencias. Es el procedimiento que sirve para registrar, analizar, diagnosticar, calificar, y seguir las incidencias que se produzcan en relación con el elemento en cuestión para darle solución.
5- Seguridad y Control. Estos procedimientos son relevantes al momento de evitar incidencias o detectarlas tempranamente.
6- Información sobre la actividad. Se refiere a la presentación de cuentas al responsable superior, así como brindar información estructurada, que sea útil para conocer la evolución de la actividad, comparar la realidad con objetivos y estándares, mejorar la calidad de la tarea y anticiparse a situaciones críticas analizando tendencias.

Es pues, la Auditoría de la Función, aplicar las ideas anteriores, al segmento de actividad al que se refirió en un principio, la Técnica de Sistemas.

El último informe de auditoría realizado, servirá para fijar objetivos concretos, comprobación de la correcta aplicación de las recomendaciones expuestas y corregir debilidades o puntos negros detectados anteriormente.

El informe final de auditoría debe reflejar la realidad contrastada, remarcando los objetivos no alcanzados, las razones expuestas por los responsables, así como nuevas recomendaciones al respecto que puedan ayudar a resolver las debilidades encontradas.

AUDITORÍA DE LA CALIDAD

La calidad se ha transformado en una necesidad de los productos y servicios que se comercializan para el cliente final. Cada vez se exige más que los productos y servicios tengan el mayor grado de calidad dentro de un precio razonable. El aforismos de ``El precio se olvida y la calidad perdura'' es cada vez más presente y exigido.

El cliente final es el mejor auditor de la calidad, al exigir el nivel que está dispuesto a pagar por la calidad misma, y no más. Por consecuencia, se debe cuantificar el nivel de calidad que se exige para poder planificar la calidad de los productos que abarcan desde, la materia prima, subproductos hasta el producto final.

Los Sistemas de Información cada vez están más presentes en esta práctica de calidad, y en todas las cosas que nos rodean y usamos. A los lugares que acudimos para adquirir, desde un servicio hasta bienes, existen los Sistemas de Información, a los cuales también se le exige buena calidad en su funcionamiento como en los bienes y servicios que adquirimos, en bancos, tiendas de autoservicio, trámites, etc.

Al decidir la fabricación de un producto de software se debe hacer una planificación, así como un Plan de Calidad específico para dicho producto.

En este plan se definen las actividades de Calidad que se tienen que realizar, los momentos de intervención de la función que asegura la calidad, la cual interviene proponiendo y supervisando los procesos de calidad a realizar en la fase de generación de todos los componentes.

Al hablar de los procesos de revisiones de calidad, existe la norma IEEE Estándar 1028 for Software Reviews and Audits, (Estándar IEEE 1028 para la Revisión y Auditoría de Software). Dicha norma tiene por objeto, definir los requerimientos para los procesos de revisión y auditoría.

Dicha norma, abarca los siguientes aspectos:

Revisión

Es la evaluación del elemento o elementos de software o del estado del proyecto que investiga las discrepancias con los resultados planificados, contando las mejoras recomendadas.

Elemento Software

Es un producto entregable o un documento producido durante el proceso o adquirido durante el desarrollo o mantenimiento del software.

Auditoría

Evalúa los productos de software, el progreso del proyecto, investiga la coincidencia con los estándares, líneas guía, especificaciones y procedimientos basados en criterios objetivos que incluyen los documentos donde se especifican:

- La forma o contenido de los productos a producir.
- Los procesos en los que los productos deben ser producidos.
- Como se debe medir la adherencia con los estándares o líneas guía.

Objetivos de las Auditorías de Calidad

Una Auditoría de Calidad tiene por objetivo, mostrar la situación real para aportar confianza y destacar las áreas que pueden afectar esa confianza. Existen diversas razones para la realización de una auditoría de este tipo:

- Establecer el estado de un proyecto.
- Verificar la capacidad de realizar un trabajo específico.
- Verificar los elementos establecidos en el Plan de Calidad desarrollados y documentados.

La auditoría deberá contar con la capacidad de investigar la pericia técnica, el desarrollo del software y la capacidad del departamento de desarrollo, el soporte del mantenimiento y la efectividad de la gestión.

Auditoría de Sistemas de Calidad de Software

El propósito de este tipo de auditoría es, proporcionar una valoración independiente sobre la conformidad de un Plan de Calidad de Software. Específicamente el objetivo es determinar, basándose en las evidencias observables y verificables. Donde la documentación del programa de calidad de software recoge los elementos básicos como mínimo, tomados del estándar ANSI/IEEE 730 u otro apropiado.

AUDITORÍA DE LA SEGURIDAD

La seguridad fue, es y seguirá siendo el área principal a auditar, ya que en algunas organizaciones, la función de auditoria informática fue creada con la principal intención de revisar la seguridad y ya después se amplió la auditoria a otras áreas.

Cada día es más importante el manejo de la información y la seguridad de la misma, haciendo énfasis en las que usan tecnologías de información para su manejo, contemplando los impactos de los fallos, accesos no autorizados, revelación de información, alteraciones en los mismos sistemas, entre otros aspectos.

Auditoría de la Seguridad Física

En esta se evalúan las protecciones físicas de datos, programas, instalaciones, equipos, redes, soportes e incluso a las personas, que estén protegidas con las debidas precauciones para evacuaciones, alarmas, salidas alternativas para minimizar así los riesgos.

Auditoría de la Seguridad Lógica

Aquí es necesario verificar los accesos permitidos y autorizados para cada usuario, según su función y con las posibilidades que el dueño haya fijado. Clasificando de manera concreta y objetiva los grupos de usuarios o sistemas, los objetivos que puedan ser accedidos con más facilidad, un disco duro, una aplicación, una base de datos, etc.

Auditoría de las Seguridad y el Desarrollo de Aplicaciones

Todas las aplicaciones y sistemas en desarrollo deben estar autorizados en distintos niveles según la importancia del desarrollo a realizar, incluso por comités en el caso de que los costes y riesgos estén por encima de algunos límites.

Auditoría de la Seguridad de los Datos

Es algo que se puede incluir en la producción y las comunicaciones, pero se debe tratar de manera particular, ya que los datos y la información son de los puntos más importantes en la organización. Los datos no solo son alfanuméricos, también son imágenes, audio, videos, entre otros, y están almacenados en diversas formas.

La protección de los datos abarca varios enfoques como: la confidencialidad, disponibilidad e integridad. En la auditoría, si se contemplan los objetivos se analizaran la destrucción de la información clasificada.

Auditoría de la Seguridad en Comunicación y Redes

En las Políticas de la organización, debe reconocerse que los sistemas, redes y comunicaciones

transmitidos y procesados son propiedad de la organización y no deberán dárseles uso sin autorización, por seguridad y productividad.

Cada usuario sólo debe recibir en el menú de opciones, lo que puede seleccionar, no más. Así mismo, lo usuarios tendrán restricciones de accesos según dominios, solo podrán ejecutar los programas autorizados y solo los técnicos autorizados podrán variar las configuraciones.

AUDITORÍA DE REDES

Para poder realizar la Auditoría de Redes, es necesario saber y utilizar el mismo vocabulario técnico que los expertos en comunicaciones manejan. Ya que con la rápida actualización de esta área, es necesario referirse a un modelo aceptado de manera común.

El modelo común que se puede tomar como referencia es, el modelo OSI (Open Systems Interconection), el cual consta de siete capas o niveles:

7- Aplicación
6- Presentación
5- Sesión
4- Transporte
3- Red
2- Enlace
1- Físico

Tienen este acomodo, porque es un modelo de niveles el cual en el proceso de transferencias, los datos deben seguir el orden de dichos niveles.

Vulnerabilidad en redes

Todos los sistemas de comunicaciones tienen un problema en común, la información que transportan viaja por lugares físicamente alejados de los responsables. Esto genera un sentido de responsabilidad en cuanto a la seguridad ya que no hay muchos procedimientos para garantizar la seguridad total de la

información.

En las redes de comunicación se han catalogado tres tipos de incidencias:

- Alteración de bits: por errores del canal de comunicación puede sufrir variaciones en parte de su contenido.
- Ausencia de tramas: por errores en los medios o equipos, algún archivo puede desaparecer en el camino de transferencia.
- Alteración de secuencia: El orden en el que se envían y se reciben las tramas no coinciden.

Por causas dolosas, y tomando en cuenta que es posible interceptar físicamente la información, existen 3 riesgos que manejar:

- Indagación.
- Suplantación.
- Modificación.

Redes abiertas (Protocolo TCP / IP)

Debido al auge de este protocolo, se llegó a la necesidad de clasificar los tipos de redes basadas en dicho protocolo:

- Intranet: Es la red interna privada y segura de la organización.
- Extranet: Es una red privada y segura interconectada en un conjunto de empresas, aunque no se usen medios transporte no seguros y ajenos como Internet.
- Internet: Es la red de redes, en donde se conecta cualquier tipo de red con el exterior de manera pública e insegura.

Auditando la Red Física

Existen varios riesgos para los datos que circulan tanto dentro como fuera del edificio, y es aquí donde se debe auditar hasta qué punto las instalaciones físicas del edificio ofrecen garantías y han sido

estudiadas las vulnerabilidades existentes.

De manera común, se supone que si no existe acceso físico desde el exterior a la red interna, las comunicaciones internas quedan a salvo. Se debe comprobar que en realidad los accesos físicos que provienen del exterior están registrados y autorizados, para evitar accesos fortuitos. A su vez, se debe comprobar que desde el interior del edificio no se intercepta físicamente el cableado.

Auditando la Red Lógica

La red permite que un equipo pueda acceder a cualquier otro, esto incluye que circule hacia el tráfico de datos hacia cualquier equipo de la red. Todo esto por medio de métodos exclusivamente lógicos, sin la necesidad de instalar algún dispositivo físicamente. Un ejemplo de ello sería que, si un equipo se dedica a enviar sin medida mensajes por la red, puede saturar el tráfico a tal grado que bloquee la red completamente, hasta llegar al resto de los equipos que conforman a la red.

Aquí es necesario monitorizar la red, revisar errores y situaciones anómalas y tener establecidos procedimientos para detectar y aislar equipos en situaciones erróneas. Si se desea que la información que viaja por la red no sea saboteada, la encriptación es la solución más adecuada.

AUDITORÍA DE APLICACIONES

Una aplicación informática o sistema de información persigue como finalidades:

- Registrar fielmente la información considerada de interés con respecto a las operaciones realizadas por una determinada organización.
- Ayudar a la realización de todos los procesos de cálculo y edición sean necesarios, partiendo de los datos registrados, permitiendo almacenar más información que la inicial.
- Facilitar la respuesta a consultas de cualquier información almacenada a quienes la precisen.
- Generar informes que ayuden a cualquier finalidad de Interés en la organización, presentando la información adecuada al solicitarla.

Etapas de la Auditoría de una Aplicación Informática

1.- Recogida de información y documentación sobre la aplicación: antes de comenzar con los trabajos de esta auditoría, se requiere de conocimientos básicos de la aplicación y su entorno, realizando un estudio preliminar en el que se obtiene toda la información que pueda ser útil para determinar los puntos débiles y aquellas funciones de la aplicación que pueda provocar riesgos. A través de entrevistas con personal usuarios de los equipos que cuentan con la aplicación, así como de toda la documentación disponible de la misma aplicación.

2.- Determinación de los objetivos de la auditoría: el examen de toda la información obtenida en el punto anterior, la identificación de puntos débiles y de las funciones críticas de la aplicación, le permitirán al auditor establecer un plan detallado del trabajo a realizar contemplando objetivos y alcances.

3.- Planificación de la auditoría: como en todo tipo de auditoría, la auditoría de una aplicación debe ser planificada con mucho cuidado. En este caso es muy importante acertar con el momento más adecuado para su realización.

4.- Trabajo de campo, informe e implementación de mejoras:

- Esta etapa consiste en la ejecución del programa de trabajo establecido, contemplando que los resultados obtenidos sobre la marcha puedan servir a ajustar el programa en función de dichos resultados.
- Aquí se recogerán las características del trabajo realizado y sus conclusiones y recomendaciones o propuestas de mejora.
- Lo que se desea alcanzar en esta etapa es, que todas las recomendaciones generadas de la auditoría, sean adoptadas como objetivos de la organización para un mejor funcionamiento.

2.7 Ética del Auditor en Informática

En el mundo actual, donde las directrices y comportamientos económicos en permanente cambio están ligados estrechamente con los avances tecnológicos, se debe de poner el control en cuanto al trato de temas relacionados con la deontología, la ética o la moral.

``Si bien la moral individual está enfatizada en forma única y personalizada, la necesidad de relacionarse y convivir unos individuos con toros en comunidad exige una cierta adaptación de las diferentes concepciones morales individuales a unas determinadas normas éticas, que facilitan una convivencia pacífica y enriquecedora común."[5]

Se tiene presente en todo momento, que mediante el ejercicio profesional, se pone de manifiesto una de las facetas de la personalidad que más incide en la valoración social de la actividad desarrollada por las personas a través de la realización de su trabajo.

Al ir planteando de forma crítica, la necesidad de sensibilizar a los auditores informáticos, integrados en un sector profesional dotado de una cierta autonomía y con características particulares, integrados de su comportamiento profesional (comportamiento técnico cualificado y comportamiento ético), se desea eliminar el falso concepto que se les tiene, ya que se piensa que su trabajo se basa solo en función de unos pocos estándares técnicos de calidad y fiabilidad dando por hecho los condicionantes éticos, que si entran en conflicto con otros condicionantes deben ser considerados como prevalentes.

Los principios éticos o deontológico aplicables a los auditores deben de trabajar en equilibrio con los del resto de profesionales y en particular con aquellos cuya actividad presente más coexistencia con la auditoría, razón por la que, junto con los principios deontológicos adoptados por distintas instituciones profesionales del entorno socio-cultural, se pueden indicar como básicos los siguientes:

1- Principio de beneficio del auditado: el auditor debe conseguir la máxima eficacia y rentabilidad de los medios informáticos, presentando recomendaciones que refuercen el sistema y el estudio de las soluciones más idóneas, según los problemas detectados, siempre y cuando las soluciones adoptadas no violen los principios éticos.

2- Principio de calidad: el auditor deberá prestar sus servicios de la mejor forma a su alcance con los medios a su alcance con libertad, en condiciones técnicas que le permitan el cumplimiento de su labor.

3- Principio de capacidad: en este caso el auditor deberá estar plenamente capacitado para su labor,

5 Auditoría en Informática, Piattini, Mario.

especialmente teniendo en cuenta que el auditado en muchas ocasiones le es difícil verificar sus recomendaciones y evaluar correctamente las mismas.

4- Principio de cautela: el auditor debe tener mucho cuidado de que sus recomendaciones estén basadas en resultados y experiencia contrastada, evitando que por intuiciones del auditor el auditado tome proyectos erróneos a futuro por los cambios de las nuevas tecnologías de la información.

5- Principio de comportamiento profesional: tanto en las relaciones con el auditado como con terceras personas, el auditor debe actuar en todo momento bajo las normas de dignidad de la profesión y de corrección en el trato personal.

6- Principio de concentración: el auditor debe evitar en todo momento que el exceso de trabajo supere sus posibilidades de concentración en su labor, ya que suele provocar la conclusión del trabajo sin las debidas garantías de seguridad.

7- Principio de legalidad: se debe evitar en todo momento utilizar los conocimientos informáticos para facilitar al auditado o terceras personas, la contravención de la legalidad vigente.

8- Principio de secreto profesional: la confidencia y la confianza sin características esenciales de las relaciones entre auditor y auditado, imponiendo obligadamente al primero, guardar en secreto los hechos e información que conozca en el ejercicio de su actividad profesional. Solamente por obligación legal se podrá omitir dicha obligación.

9- Principio de veracidad: el auditor está obligado a tener veracidad en todo momento con el auditado, referente a las manifestaciones del trabajo realizado, con los límites impuestos por los deberes de respeto, corrección y secreto profesional.

10- Principio de discreción: el auditor deberá mantener discreción en la divulgación de datos, que se le hayan puesto de manifiesto durante la ejecución de la auditoría.

CAPÍTULO 3

Metodologías para el desarrollo de Auditoría en Informática

3.1 Metodología para el desarrollo de una Auditoría en Informática de Mario Piattini

Mario Gerardo Piatinni Velthuis, doctor Ingeniero en informática por la Universidad

Politécnica de Madrid.

Máster en Auditoría en informática (CENEI).

Especialista en la aplicación de Tecnologías de la Información a la Gestión
Empresarial (CEPADE-UPM).

CISA (Certified Information System Auditor) por la ISACA (Information System Audit
and Control Association).

Diplomado en Psicología (UNED).

Ha sido director del departamento de desarrollo de la empresa SIE y socio fundador de Cronos Ibérica, S A en la que ha sido director de los departamentos de Formación y Metodologías e Investigación y Desarrollo.

Ha trabajado como consultor y profesor para numerosos organismos y empresas, entre las que destacan:
Ministerio de Industria y Energía, Ministerio de Administraciones Públicas,
Ministerio del Interior, Siemens-Nixdorf, Unisys, Hewlett-Packard, Oracle, ICM, etc.

Actualmente es profesor titular en la Escuela Superior de Informática de la Universidad de Castilla-La mancha en ciudad Real, donde dirige el grupo de investigación Alarcos, especializado en Sistemas de Información, Base de datos e Ingeniero de Software.

Piatinni opina que existen diferencias entre el control informático y la Auditoría Informática:
El control informático debería ser independiente del departamento controlado. Ya que ``por segregación

de funciones la informática no debería controlarse así misma". Partiendo de la base de un concepto en el que la seguridad de sistemas abarca un campo mucho mayor de lo que es la seguridad lógica, podríamos decir que:

- El área informática implementa los procesos informáticos seguros.
- El control interno implementa los controles.
- La Auditoría Informática evalúa el grado de control.

Conociendo este punto de vista de Piatinni, podríamos decir que existen diferencias muy marcadas entre las funciones de control informático y las de auditoría en Informática.

Mencionaremos las funciones que Piatinni describe tanto para la Auditoría en Informática como para el control interno Informático, ya que de este punto partiremos a la metodología que él realiza.

La Auditoría Informática.

- Tiene la función de vigilancia y evaluación mediante dictámenes, y todas sus metodologías van encaminadas a esta función.
- Tiene sus propios objetivos distintos a los auditores de cuenta, aunque necesarios para que éstos puedan utilizar la información de sus sistemas para sus evaluaciones financieras y operativas.
- Evalúan eficiencia, costo y seguridad en su más amplia visión.
- Operan según el plan auditor
- Utilizan metodologías de evaluación del tipo cualitativo con la característica de las pruebas de auditoría.
- Establecen planes quincenales como ciclos completos.
- Sistemas de evaluación de repetición de la auditoría por nivel de exposición del área auditada y el resultado de la última auditoría de esta área.
- La función de soporte informático de todos los auditores.

Control Interno Informático.

- Tiene funciones propias (administración de la seguridad lógica, etc.).
- Funciones de control dual con otros departamentos.
- Función normativa y del cumplimiento del marco jurídico.
- operan según procedimientos de control en los que se ven involucrados y que luego se desarrollarán.
- Al igual que la auditoría y de forma opcional pueden ser el soporte informático de control interno no informático.

Son una gran cantidad de funciones para desarrollarlas desde el inicio de la implementación, pero nos sirve conocerlas para no perder el objetivo que considera Piatinni: El control informático es el componente de la actuación segura entre los usuarios, la informática y control interno, todo esto auditado por los auditores de informática.

Expliquemos que Piatinni maneja 2 metodologías para poder cubrir los 2 aspectos más importantes que el maneja:

1. Clasificación de la Información y
2. Procedimientos de Control.

1. Para la clasificación de la Información maneja la metodología de PRIMA la cual define en:

- Estratégica (información muy restringida, muy confidencial).
- Restringida (a los propietarios de la información).
- De uso interno (a todos los empleados).
- De uso general (sin restricción).

2. Para la obtención de control maneja otra metodología `` la obtención de los procedimientos de Control", esta metodología nos ayuda a saber si es suficiente y como mejorar el control informático.

Estas dos metodologías son las que Piatinni considera para la relación de la Auditoría Informática, desde mi punto de vista observo que el tener metodologías para trabajar propicia que a una se le dé más

importancia que a la otra; Para Piatinni es de suma importancia el control interno.

3.2 Metodología para el desarrollo de una Auditoría en Informática de José Antonio Echenique

José Antonio Echenique García, secretario adjunto de la facultad de Contabilidad y Administración de la Universidad Nacional Autónoma de México.

Una parte muy importante que se manejan de manera muy cuidadosa y detallada es la planeación de la Auditoría en Informática, para Echenique ésta debe de contener:

- Objetivos.
- Revisión preliminar
- Revisión detallada
- Examen y evaluación de la información.
- Pruebas de controles del usuario.
- Pruebas sustantivas.
- Evaluación de los sistemas de acuerdo al riesgo.
- investigación preliminar.
- Personal participante.

y la metodología que Echenique maneja están los siguientes puntos:

1. Para la evaluación de la dirección de informática se llevarán a cabo las siguientes actividades:

- Solicitud de los manuales administrativos, organización, funciones, planes, políticas, estándares utilizados y programas de trabajo.
- Solicitud de costos y presupuestos de informática.
- Elaboración de un cuestionario para la evaluación de la dirección.
- Aplicación del cuestionario al personal y realización de entrevistas.
- Entrevistas a líderes de proyectos y a usuarios más relevantes de la dirección de informática.

- Análisis y evaluación del informe.
- Elaboración del informe.

2. Para la evaluación de los sistemas tanto de operación como en desarrollo, se llevaran a cabo las siguientes actividades:

- Estudios de viabilidad y costo / beneficio.
- Solicitud de análisis y diseño de los sistemas en operación y en desarrollo.
- Solicitud de documentación de los sistemas en operación (manuales técnicos de operación, de usuario, diseños).
- Solicitud del plan de trabajo.
- Solicitud de contratos de compra o renta de software.
- Solicitud de licencias y derechos de autor.
- Plan de contingencia y recuperación en caso de desastre.
- Recopilación y análisis de los procedimientos administrativos de cada sistema.
- Análisis de base de datos.
- Análisis de la seguridad lógica y confidencialidad.
- Evaluación de los proyectos en desarrollo, propiedades y personal asignado
- Evaluación de la participación de auditoría interna
- Evaluación de las licencias, la obtención de derechos de autor y de la confidencialidad de la información.
- Entrevistas con los usuarios de los sistemas.
- Evaluación directa de la información obtenida contra las necesidades y requerimientos de los usuarios.
- Análisis objetivo de la estructuración y flujo de los programas.
- Análisis y evaluación de la información compilada.
- Elaboración de informe.

3. Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:

- Solicitud de los estudios de viabilidad, costo / beneficio y características de los equipos

actuales, proyectos sobre adquisición o ampliación de equipo y su actualización.

- Solicitud de contratos de compra o renta de los equipos.
- Solicitud de contratos de mantenimiento de los equipos.
- Solicitud de contratos y convenios de respaldo.
- Solicitud de contratos de seguro.
- Bitácoras de los equipos.
- Elaboración de cuestionario sobre la utilización de equipos, archivos, unidades de entrada / salida, equipos periféricos y su seguridad.
- Visita a las instalaciones y a los lugares de almacenamiento de archivos.
- Evaluación técnica del sistema eléctrico y ambiental de los equipos y en general de las instalaciones.
- Evaluación de los sistemas de seguridad de acceso.
- Evaluación de la información\'n recopilada, obtención de gráficas, porcentajes de utilización de los equipos y justificación.
- Elaboración del informe.

4. Elaboración del informe final, presentación y discusión del mismo y presentación de conclusiones y recomendaciones.

Para Echenique la alta dirección juega un papel importante, ya que es en la alta dirección donde se toman las decisiones de un proyecto de auditoría, de esta manera Echenique nos muestra en su libro un ejemplo de propuesta de servicios de auditoría en informática.

La metodología de Echenique es muy concreta, se basa en los objetivos de la auditoría en Informática logrando así la auditoría de los sistemas en operación como en desarrollo, evalúa los equipos, se presenta reporte final incluyendo conclusiones y recomendaciones.

Para una empresa que busca eficiencia, esta es una metodología que pudiera acoplarse más para una Auditoría en Informática.

CAPÍTULO 4

Metodología propuesta

4.1 Metodología propuesta de tesis

Este capítulo está dedicado a la formulación de una propuesta de metodología que nos proporcione la eficiencia necesaria para llevar a cabo una auditoría en Informática con éxito para ello debemos tener en cuenta que el proceso que se lleva a cabo para lograr nuestros objetivos debe ser llevado a la práctica para que se cumpla el tiempo programado, los costos estipulados así como los resultados esperados.

Cabe mencionar que esta propuesta metodológica ha sido considerada para tamaños de empresas diferentes tales como pequeñas, medianas y grandes; y se basa en las propuestas expuestas en el capítulo precedente, Toda empresa sin tomar en cuenta su tamaño requiere de Auditoría en Informática para poder maximizar la tecnología, métodos y manejo de información entre otros.

Una empresa pequeña, requiere de una amplia supervisión y manejo para poder desarrollarse, la empresa mediana también requiere de esto y agregar tecnología y la empresa grande ya habiéndose desarrollado, con utilización de tecnología de punta buscará la eficiencia de cada uno de los equipos de cómputo y aplicaciones cuales quiera que maneje.

Proponiendo así esta metodología la cual será ajustada a las necesidades requeridas de la empresa, existiendo el paso de adaptación donde se consideran las características de la empresa.

Se recomienda el seguimiento en orden de esta metodología para obtener los resultados de cada fase y lograr llevar acabo la auditoría en informática de la empresa elegida.

Conociendo los puntos más importantes podremos sugerir lo siguiente:

Metodología para el desarrollo e implementación de la auditoría en informática en busca de la eficiencia. Las etapas que lleva son:

1. Etapa de Pre-Auditoría

Cuando un auditor es solicitado por alguna empresa, este no tiene un conocimiento de la misma, para

esto requiere un tiempo, para conocer puntos muy específicos y así el auditor realice un diagnostico el cual se examinen las funciones y actividades generales de la Informática, en la organización.

2. Etapa de inicio

En esta etapa se justifica la revisión o evaluación de las áreas o funciones críticas relacionadas con la informática.

Esta fase involucra la autorización de la alta dirección, el objetivo primordial es la justificación del desarrollo del proyecto con base en todos los argumentos y detalles encontrados, analizados en las fases anteriores.

3. Etapa de análisis

Lo primero es llevar un análisis detallado del proyecto a entender, para esto debemos dar a conocer los objetivos generales y particulares del cliente, de forma que las metas fijadas puedan ser cumplidas.

Los resultados de esta fase son la comprensión y detalle de nuestros objetivos así como las metas de modo que se cubran los requerimientos del cliente.

4. Etapa de desarrollo

Esta fase es la más importante ya que da inicio a la parte práctica del proyecto, en esta etapa es donde el auditor pone de manifiesto todos sus conocimientos, profesionalismo, técnicas, experiencia profesional, ética, etc.

Se ejecutan tareas de acuerdo con el plan detallado, respetando el proceso metodológico y coordinando los recursos humanos con eficiencia, documentar entrevistas, visitas, cuestionarios, etc., para poder lograr una eficiencia en cada una de las actividades realizadas por el auditor en informática.

5. Etapa final

Una vez que el proyecto de Auditoría se termina, se elabora un documento final, en el cual se expliquen los objetivos, observaciones, recomendaciones y conclusiones del proceso.

La característica más importante que debe cubrir este informe es la veracidad de la información para que tanto las consideraciones y conclusiones que se ofrezcan sean con la certeza de que los datos son reales y de buena fuente.

En el informe final ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

CAPÍTULO 5

Conceptos de Ingeniería de Software.

5.1 ¿Que es la Ingeniería de Software?

Actualmente las Organizaciones y Empresas, así como la Economía de los países desarrollados tienen una necesidad muy alta de Software, que les ayude a la hora de la administración y la gestión.

La Ingeniería de Software consta de consta de teorías, métodos y herramientas para el desarrollo profesional de software. Otorgando así, una ayuda efectiva en el incremento de ingresos, tanto organizacionales, como nacionales.

La Ingeniería de Software está compuesta por una serie de modelos que abarcan los métodos, herramientas y procedimientos. Dichos modelos son llamados ``paradigmas de la Ingeniería de Software", que a su vez se eligen de acuerdo al tipo y aplicación del proyecto, controles y entregas a realizar.

El proceso de construcción de un producto de software se conforma de algunas etapas, que abarcan desde la obtención de requisitos, el diseño del sistema, la codificación y pruebas del sistema. Donde se parte de una necesidad específica, para así averiguar dichos requisitos y hasta la implementación del mismo sistema.

A todas estas etapas y procesos se le conocen como Ciclo de vida del sistema. El cual se puede determinar que comienza en la concepción de la necesidad, pasando por su construcción, la implementación, su mantenimiento y actualizaciones, hasta sus desinstalación en el caso de no ser más funcional.

Existe una clasificación de productos de software:

- Productos genéricos: estos son producidos por alguna organización para ser vendidos en el mercado.
- Productos hechos a medida: estos son desarrollados bajo pedido a un desarrollador específico.

Por lo regular se opta por productos genéricos, pero las ventajas están en los productos hechos a medida, debido al esfuerzo que se les pone al momento de su desarrollo.

5.2 Características de los productos de Ingeniería de Software

Debido a que los productos de software deben ser elaborados bajo normas y leyes que cumplan con estándares de funcionalidad y calidad, estos deben de contar con ciertas características, que estén dentro de las normas y que permitan explotar dicha calidad. Las características son las siguientes:

- Mantenibles: se refiere a que los productos de software, a pesar de su construcción hecha a la medida, estos deberán ser capaces de evolucionar y crecer, y seguir cumpliendo los requerimientos establecidos.
- Eficientes: los productos deberán cumplir con lo que se les ordene de manera eficiente, sin desperdiciar ni consumir de más los recursos del sistema ni de los equipos.
- Confiabilidad: se debe de hacer un sistema que no permita el daño físico o económico en el caso de tener alguna falla de cualquier tipo.
- Utilización adecuada: el sistema deberá contar con una interfaz adecuada, entendible y manejable para el usuario, así como la documentación necesaria para su operación.

Algunos aspectos que hay que cuidar con respecto a estas características son:

- La importancia es relativa en cuanto a las características del sistema, ya que varía desde el tipo de producto hasta el ambiente en el que será utilizado.
- Algunas de las características podrán ser más importantes según sea el caso y lugar en que se use el sistema. Es decir, que en un sistema de seguridad pueden predominar la confiabilidad y la eficiencia.
- Los costos varían según el grado de importancia que se le dé a cada una de las características.

El proceso de la construcción de software son actividades estructuradas en conjunto, que ayudan al desarrollo de un sistema de software, como la especificación, el diseño, la validación y la evolución. Estas actividades varían según la organización y el tipo de sistema solicitado. Así también existen características que se deben tomar muy en cuenta en dicho proceso que contesten a ciertas preguntas:

- Entendible: ¿El proceso es entendible y bien definido?
- Visible: ¿El proceso ser visible al exterior?
- Soportable: ¿El proceso puede ser soportado por herramientas CASE?

- Confiable: ¿Los errores en el proceso son detectados antes de que sean del producto?
- Robusto: ¿El proceso puede continuar aun con problemas inesperados?
- Mantenible: ¿El proceso puede evolucionar para cumplir objetivos?
- Rapidez: ¿Qué tan rápido se puede producir el sistema?

Modelo de Ingeniería del proceso

Así como existen las características que se deben cumplir al momento de desarrollar un sistema o producto de software, existe un modelo a seguir para lograr que el sistema cumpla con los objetivos establecidos de la organización:

- Especificación: aquí se establecen los requerimientos y restricciones del sistema.
- Diseño: se produce un modelo del sistema en papel.
- Manufactura: aquí se construye el sistema.
- Prueba: se verifica que se cumplan las especificaciones requeridas.
- Instalación: se entrega el sistema al usuario asegurando su operacionalidad.
- Mantenimiento: aquí se reparan las fallas en el sistema cuando son detectados.

5.3 Modelos que maneja la Ingeniería de Software

La Ingeniería de software se compone de una serie de modelos o paradigmas de desarrollo de software, que a su vez contemplan los métodos, las herramientas y procedimientos con los que se realizara el software. La elección de alguno de los modelos dependerá del tipo de proyecto, de la aplicación, los controles y las entregas que se deberán realizar.

Para la construcción de un sistema de software se requiere de un proceso. Dicho proceso se puede concretar a los pasos que empiezan desde la obtención de requisitos del software, hasta la instalación con su debido mantenimiento y actualizaciones. Dicho proceso se desenvuelve por una serie de etapas llamadas en conjunto ``ciclo de vida" del sistema de software. Dicho ciclo establece el orden de las etapas del proceso del software y los criterios a contemplar para poder avanzar de etapa en etapa.

Las etapas del ciclo de vida del proceso de desarrollo del software son las siguientes:

- Especificación del software, donde los clientes e ingenieros definen el software a producir y las restricciones sobre su operación.
- Desarrollo del software, en esta parte el software se diseña y se programa.
- Validación del software, aquí el software se válida para asegurar que es lo que el cliente requiere.
- Evolución del software, donde se modifica para adaptarlo a los cambios requeridos por el cliente y el mercado.

Según la norma de la IEEE 1074, el ciclo de vida se define como ``una aproximación lógica a la adquisición, el suministro, el desarrollo, la explotación y el mantenimiento del software". En tanto la norma ISO 12207 dice que, ``el modelo del ciclo de vida es el marco de referencia, que contiene los procesos, las actividades y las tareas involucradas en el desarrollo, la explotación y el mantenimiento de un producto de software, abarcando la vida del sistema desde la definición de requisitos has la finalización de su uso". En ambas reglas se consideran a una actividad como un subconjunto de tareas y una tarea como una acción que transforma las entradas y salidas según Mario Piattini.

Como bien se ha mencionado, los modelos de procesos de software son una descripción simplificada del desarrollo de software. Estos modelos pueden incluir actividades que son parte de los procesos y productos de software y el papel de las personas involucradas en la ingeniería de software. Algunos ejemplos son:

1 Modelo de flujo de trabajo: que muestra la secuencia de actividades en el proceso (entradas, salidas y dependencias), las actividades aquí representan acciones humanas.

2 Modelo de flujo de datos o de actividad: este representa el proceso como conjunto de actividades, donde cada una realiza una transformación en los datos, como la entrada de una especificación se convierte en un diseño de salida. Pueden representar transformaciones hechas por personas o computadoras.

3 Modelo de rol / acción: muestra los roles y actividades de las personas involucradas en el proceso del

software junto con sus responsabilidades.

Existen tres modelos o paradigmas generales de desarrollo de software que contemplan todas las actividades anteriores y de los cuales se pueden hacer mezclas según el tamaño y complejidad del software para un mejor desarrollo del mismo. Estos modelos son los siguientes:

Modelo de Cascada: este modelo considera todas las actividades anteriores y las presenta como fases del proceso por separado de forma lineal, a su vez permitiendo iteraciones con la fase anterior para poder hacer alguna corrección. Una vez aprobada cada una de las fases se continúa con la siguiente hasta cumplir con todas las fases.

El número de fases puede variar según la dimensión de los requerimientos del software pero por lo general se presentan las siguientes fases:

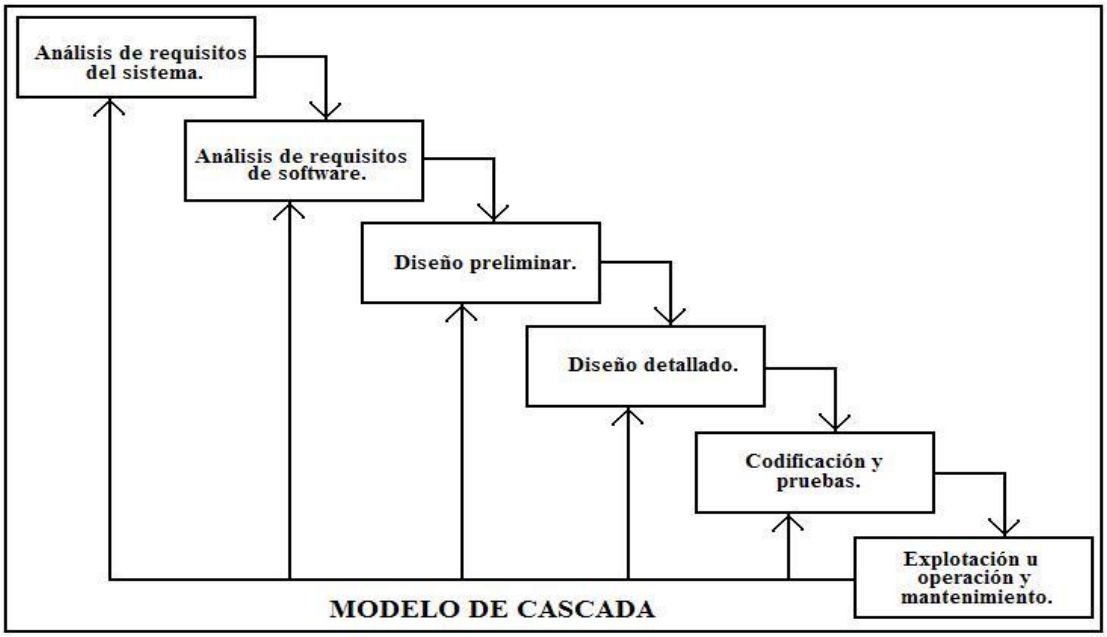
- Análisis de requisitos del sistema.
- Análisis de requisitos de software.
- Diseño preliminar.
- Diseño detallado.
- Codificación y pruebas.
- Explotación u operación y mantenimiento.

Este modelo cuenta con las siguientes características:

- Una vez terminada una fase, se puede continuar con la siguiente.
- Es útil como control de fechas de entregas.
- Al final de cada fase el personal de creación del software así como los mismos usuarios tiene la oportunidad de revisar el progreso del proyecto.

Este modelo también presenta algunas críticas, las cuales son necesarias de mencionar para un mejor uso del mismo. Se sostiene que los proyectos reales rara vez siguen una línea como tal, es decir, que se presentan iteraciones que van más allá de la etapa anterior. Como el sistema no estará en funcionamiento hasta haberse finalizado el proyecto, el usuario recibe el producto ya que se han

consumido todos los recursos.



Desarrollo Iterativo: en este modelo las fases de desarrollo de software son las mismas a las del modelo de cascada. En cada fase siguiente se agregan al sistema nuevas funciones y requisitos que permitan el perfeccionamiento a partir de una versión previa. Este modelo es más efectivo cuando los requisitos presentan ambigüedad e imprecisión, ya que permite un refinamiento, que lleve a una ampliación de los requisitos y especificaciones derivadas de la fase anterior.

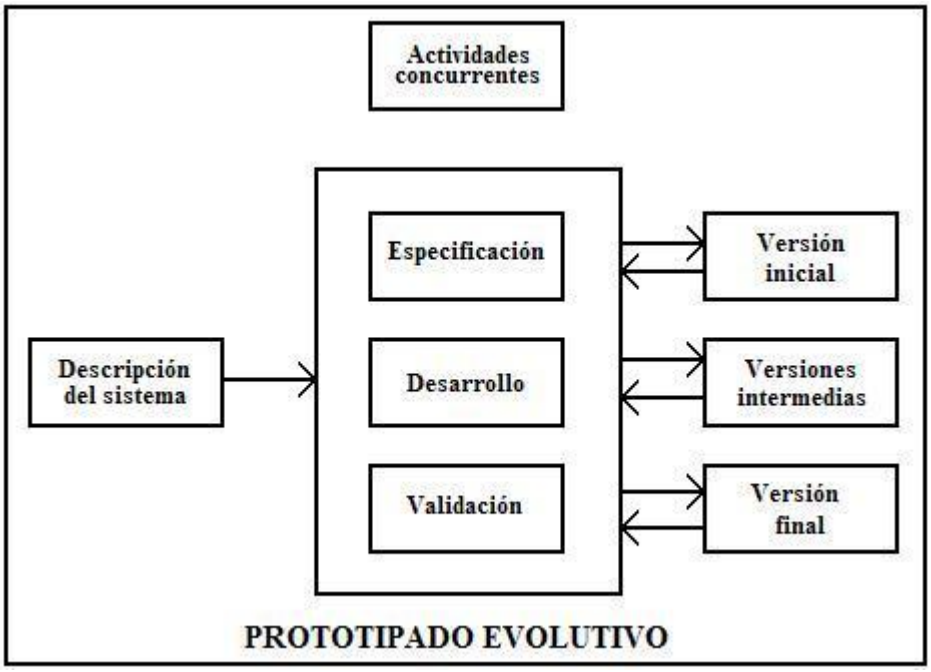
Un defecto de este modelo podría ser la detección tardía de requisitos habiendo avanzado en un número considerable de fases, haciendo su corrección tan costosa como en el modelo de cascada.
Prototipado Evolutivo: este modelo tiene como principal intención de ayudar a comprender los requisitos que presenta el usuario, apoyando en los casos en que el usuario no tenga aun las ideas claras de lo que solicita. A su vez, ayuda al ingeniero en casos de que presente dudas en la solución pensada.

Al usar este modelo se da una modificación en las fases del modelo clásico de cascada, resultando como sigue:

- Análisis de requisitos del sistema.
- Análisis de requisitos de software.
- Diseño, desarrollo e implementación del prototipo.

- Prueba del prototipo.
- Refinamiento de las especificaciones del prototipo.
- Diseño e implementación del sistema final.
- Explotación u operación y mantenimiento.

Existen muchos casos en los que se pueden usar prototipos descartables para esclarecer los detalles y aspectos del sistema que aún no se entienden bien, pero conlleva sus riesgos como, la falta de visibilidad al momento de ir haciendo paso a paso las actividades de cada fase, que pueden generar retrasos o trabajo lento.



Modelo de Espiral: este modelo reúne y combina las características y fases de los modelos anteriores, añadiendo al mismo tiempo nuevos elementos propios que ayudan a una mejor organización y mejores resultados al momento de la creación del software.

Se definen cuatro actividades en este modelo en cuatro cuadrantes, los cuales indican cada una de las etapas de la creación del software en cada una de las iteraciones de la espiral:

1 Planeación: aquí se identifican los objetivos específicos de cada fase del proyecto, así como las

alternativas y las restricciones.

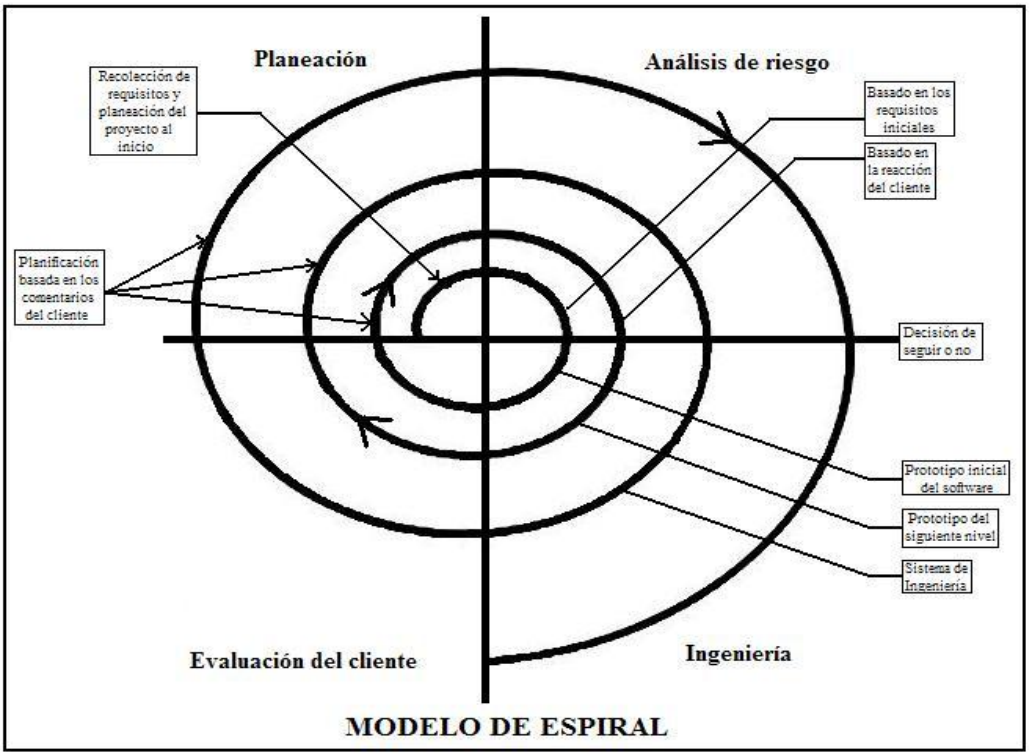
2 Análisis de riesgos: se da una identificación y resolución de los riesgos que pueden hacer fracasar al proyecto y así minimizarlos.

3 Ingeniería (desarrollo y validación): se elige el modelo adecuado para la siguiente fase del desarrollo.

4 Evaluación: se evalúan los resultados de ingeniería y se trazan planes para la siguiente iteración de la espiral.

Con cada iteración de la espiral se construye una versión sucesiva del software cada vez más completas. A su vez se enfrenta a que muchas veces se requiera de mucha habilidad para valorar los riesgos para que no surjan problemas.

Algunas de las ventajas más importantes que presenta este modelos contemplan su centro de atención en la reutilización de componentes y eliminación de errores en información en fases iniciales, integra desarrollo con mantenimiento y provee un marco de desarrollo de hardware / software.



MODELO DE ESPIRAL

CAPÍTULO 6

Tecnologías Web y Software para trabajo en grupo WorkGroup

6.1 Tecnologías Web, características.

Las tecnologías Web son aquellas que utilizan las técnicas, métodos y formas para la interconexión de equipos de cómputo, así como de las tecnologías de presentación, configuración e implementación de páginas Web, haciendo más fácil el uso y el acceso para los usuarios.

Debido al rápido crecimiento de la WWW (World Wide Web), al uso cada vez más indispensable del HTML, para proveer de información más rápida y a la mano de los usuarios a través de páginas web, a la amplia variedad de herramientas, protocolos, recursos e infraestructura y a la debida estandarización de todo lo antes mencionado, se tiene la necesidad de ver y aprovechar todo esto de manera más fácil, sencilla y cómoda para el usuario.

Así se llega a las tecnologías Web, que son todas aquellas que utilizan todas las tecnologías de interconectividad de ordenadores y la presentación de información en la red, todo esto a través de páginas Web.

En la actualidad gracias al uso masivo de estas tecnologías se tiene una gran variedad de herramientas para la creación de las mismas, haciendo de esto un solo campo de estudio de todas las especializaciones de las aplicaciones de tecnologías de comunicación, que permiten el desarrollo de sistemas web.

El objetivo principal que persiguen las tecnologías web es el de permitir el intercambio de información en diversos tipos, a una escala de nivel mundial de acceso fácil para los usuarios. A su vez ponen a disposición una serie de funcionalidades básicas desde centros educativos, hogar y lugar de trabajo, que permiten nuevas posibilidades de desarrollo personal y de manejo de las actividades familiares, laborales, empresariales y de formación.

Las funciones principales que presentan las tecnologías web contemplan: la facilidad en la búsqueda de información, la obtención de diversos materiales educativos en línea, proporcionar información relacionada con actividades de centros educativos, ampliar y facilitar la comunicación entre personas, publicaciones en Internet, facilitar la gestión administrativa y comercial, proporcionar publicidad, entretenimiento y motivación.

Para que las tecnologías web funcionen de manera eficiente y completa se requieren de los siguientes componentes y tecnologías básicos:

- Navegadores Web: son las aplicaciones (programas) que permiten la visualización grafica de las páginas Web. Muestran el resultado de utilizar lenguajes de hipertexto como lo es HTML, permitiendo visualizar diferentes fuentes de texto, imágenes, video y escuchar sonidos. Ejemplos de estos navegadores son; Internet Explorer, Mozilla Firefox, Opera, Netscape Navigator, Safari, etc.
- Servidores Web: son programas que implementan el protocolo HTTP (HiperText Transfer Protocol), diseñados para la transferencia de páginas Web, así como archivos y datos solicitados por un cliente. Algunos ejemplos de estos servidores son; Apache, Internet Information Services IIS, Resin, Tomcat, etc.
- Otras tecnologías y herramientas: aquí se presenta una serie de con combinaciones entre tecnologías de programación de páginas Web con distintos lenguajes de etiquetas y programación, así como de sistemas gestores de bases de datos que permiten la transferencia más efectiva de diversos tipos de archivos e información solicitada en la red.

Por la gran diversidad de herramientas y tecnologías que integran un buen manejo de la información en la red, hoy en día se tiene un uso y una necesidad cada vez más fuerte de las tecnologías de información, por su manejabilidad, accesibilidad y eficiencia. A continuación se muestran las tecnologías de información usadas en este trabajo de tesis.

6.2 Lenguajes de marcado, HTML, XML y XHTML.

HTML

Las siglas HTML significan HiperText Markup Language, es decir, que es un lenguaje que permite la creación de páginas Web usando etiquetas de hipertexto, dando a estas páginas características, formato y ventajas al introducir texto común sin formato en el archivo fuente, que será interpretado por el navegador Web.

Todos los navegadores Web leen texto común y corriente, pero al utilizar el lenguaje de marcado

HTML, se le da grandes ventajas como efectos en el texto, imágenes, enlaces a otras páginas y archivos, así como aplicaciones multimedia, etc.

Al momento de la creación del lenguaje, se ideo que fuera 100\% portable, es decir, que pudiera ser leído y visualizado independientemente del sistema operativo instalado en el equipo. Sería perfecto hacer una página HTML en una computadora con sistema operativo DOS para luego ser montada en un servidor HTML con sistema operativo UNIX, y pueda ser visto por personas que incluso utilicen sistema operativo MAC OS. Esto se debe a que todo el contenido de la página es texto, en formato ASCII, estándar de texto interpretado en todos los tipos de sistemas operativos.

Gracias a la difusión masiva de Internet hoy en día, el desarrollo de documentos y páginas en HTML tiene un uso constante e imparable, mediante el acceso a los servidores Web. Mediante este servicio se pueden elaborar aplicaciones de todo tipo, desde bases de datos hasta aplicaciones multimedia y más a nuestro alcance.

Existen programas y herramientas que ayudan a la creación e documentos en lenguaje HTML, pero basta con un simple editor de texto y nuestra imaginación para la creación de una página Web de lo más completa.

La sintaxis en los comandos de HTML es muy sencilla, para el uso de una etiqueta generalmente se usan los conocidos containers o signos de mayor y menor que < > que nos indican el comienzo y el fin del formato que se le dará al texto o la información propia del documento que se encuentra contenida en esa etiqueta.

Un ejemplo esencial seria el que nos indica el comienzo y el fin del documento escrito en HTML, < HTML> seria el comienzo del documento y con < /HTML> seria el fin del documento que genera la página Web. Casi todos los comandos tienen esta estructura en su sintaxis, salvo algunos como < BR> que nos indica un punto y aparte.

Algo peculiar de este lenguaje es que en el documento fuente un espacio en blanco no es nada, es decir, que si se ponen 4 o 5 espacios en blanco seguidos, serán interpretados como uno solo por el navegador Web, en el caso de ser solo texto.

Una recomendación importante que hace la W3C, World Wide Web Consortium, organismo regulador de este lenguaje, y en conjunción con grandes compañías como Netscape, Microsoft, Novell, etc. se hace obligatoria la inclusión al comienzo del documento antes de la declaración < HTML > la etiqueta < !DOCTYPE HTML PUBLIC ``//W3C//DTD HTML 4.01 Final//EN"> , que básicamente se interpreta en la página Web el tipo de documento, que es público, el consorcio del estándar, la versión del lenguaje y el idioma que contiene el documento, con el fin de identificarlo.

XML

XML es un estándar internacional desarrollado por el Comité de Revisión Editorial de SGML, creado bajo el patrocinio del W3C en 1996, el cual hace una recomendación oficial en el sitio Web http://www.w3.org/TR/2000/REC-xml-20001006 que dice textualmente; "El Lenguaje Extensible de Marcas, abreviado XML, describe una clase de objetos de datos llamados documentos XML y parcialmente describe el comportamiento de programas de computador que pueden procesarlos".

Desglosando esta recomendación en varias ideas que puedan ayudar a entender este lenguaje se explica como sigue:

- Marcas o marcado: son señales con un propósito definido que se añaden a un texto para ayudar a su procesado.
- Extensible: ser refiere a que se pueden definir las marcas como se desee, siempre pensando en la función que pueden desarrollar para no trabajar sin sentido. Se ha diseñado para adaptarse a una gran cantidad de diversas situaciones, según los conocimientos de la persona que lo emplea logrando documentos tan sencillos como complejos.
- Las clases de objetos se refiere a una gran cantidad de tipos de fuentes de información, bases de datos, documentos de texto, códigos fuentes, etc.
- En cuanto a la expresión ``parcialmente describe" indica que XML se utiliza para describir datos pero no se utiliza para describir que hacer con esos datos.

XML ofrece ventajas y aportaciones que amplían el campo de trabajo y enriquecimiento del documento que se está creando, de las más importantes se señalan, la independencia de los datos respecto de las

aplicaciones, información sobre la información, un contexto extremadamente útil en su procesado informático y los elementos para describir la estructura de un documento.

XHTML

Con HTML 4.0 se alcanzó la cima en lo que respecta a nuevas etiquetas HTML, se terminó la competencia entre fabricantes de navegadores por patentar nuevas funciones y etiquetas. Con HTML 4.01 solo se realizaron correcciones de redacción y las futuras ampliaciones y novedades aparecen en el entorno XML. Mientras que HTML contiene una cantidad concreta de etiquetas definidas, XML permite a cada usuario definir sus propios elementos (homólogos a HTML).

Como consecuencia XML diversifica mucho su ámbito de aplicación, por otra parte no se puede prescindir de HTML cuando se trata de publicar unas pocas páginas. Por lo tanto se presenta una cooperación entre ambos lenguajes y fabricantes de navegadores como Microsoft ya ofrecen soporte muy completo para XML en páginas HTML. En XHTML simplemente se ha redefinido HTML 4.0 con las reglas de XML.

Al adaptar documentos HTML a la norma XHTML se podrá fijar el grado con que el documento se atiene a las reglas XHTML. Esto se logra a través de las siguientes definiciones !DOCTYPE al inicio del documento HTML:

```
< !DOCTYPE html PUBLIC``-//W3C//DTD XHTML 1.0 STRICT//EN"
 ``http://www.w3.org/TR/xhtml1/DTD/strict.dtd" >
< html xmlns=``http://www.w3.org/TR/xhtml1" >
< head >
< title > Documento XHTML < /title >
< /head >
< body >
< p > Desde aquí se va a la página de W3C
< a href=``http://www.w3c.org" > W3C < /a > < /p >
< /body >
< /html >
```

Este es un pequeño ejemplo de la estructura de un documento HTML que incluye código XHTML.
El principal requisito de XHTML dirige la mirada hacia XML, que exige que los documentos estén bien formados (wellformed). Se entiende por bien formados a que los documentos deben respetar ciertas reglas observadas en XML, a diferencia de que HTML no toma muy en cuenta algunas formas. Como principales requisitos se tiene que; las etiquetas se deben intercalar correctamente, por ejemplo la expresión < p > un texto en < em > negrita < /em > < /p > es correcta, mientras que < p > un texto en < em > negrita < /p > < /em > no esta permitida. Se debe llevar un orden entre etiquetas iniciales y finales según como se hayan escrito.

En XML es obligatorio escribir en minúsculas los nombre de todas las etiquetas y atributos y por ello en XHTML también se debe respetar dicha regla. Así como las etiquetas no vacías deben tener siempre una pareja de cierre, la formación permitida en HTML < ep > no esta permitida ya que solo refiere a un nuevo párrafo pero no tiene una etiqueta que la cierre.

6.3 Lenguaje Script PHP

PHP es un lenguaje de programación creado inicialmente como herramienta para el desarrollo de aplicaciones Web. Permite el diseño de páginas dinámicas de servidor, capaces de responder de forma inteligente a las demandas de cualquier cliente, permitiendo la automatización de muchas tareas. Siendo este uno de los lenguajes más usados por parte del servidor en el desarrollo de páginas dinámicas.

PHP proporciona una combinación de varias características que lo hacen uno de los más utilizados, entre las más notables esta la de ser un software de libre distribución y multiplataforma, pudiendo ser instalado en distintos sistemas operativos, siguiendo la filosofía opens urce. Además de permitir la comunicación con bases de datos, comunicación vía sockets, generación de gráficos, etc.

En sus comienzos PHP era un conjunto de scripts escritos en lenguaje Perl, que permitían el control de los accesos a las páginas personales de su creador, Rasmus Lerdorf, llamándolo Personal Home Page Tools. Paulatinamente fue completando las funcionalidades básicas escribiendo programas en C.

Tras dejar abierto el código fuente escrito en C para la colaboración en su mejora se dio una reescritura en su núcleo por parte de dos colaboradores, que le dieron un nuevo motor llamado Zend (acrónimo de los apellidos Zeev y Andi), usado en la versión PHP 4.0, con las características más reconocidas como, dar soporte a la mayoría de los servidores Web, facilidades de orientación a objetos, más seguridad en el control de entradas de usuarios, etc.

La versión más actual de PHP es la 5.0, basada en el nuevo motor Zend 2 reescrito en su totalidad, pero que otorga dentro de sus características más notables, la de un soporte más completo para la programación orientada a objetos. Incorpora la gestión de excepciones, soporte nativo para el sistema gestor de bases de datos MySQL, la cual, además de la interfaz habitual, encierra una interfaz basada en objetos.

Además de permitir la escritura de scripts para ser ejecutados en servidores Web, puede ser usado como cualquier otro lenguaje para escribir programas que se ejecuten sin la necesidad de estar conjuntamente en un servidor Web. A la par de permitir todas las acciones propias de un script CGI (procesamiento de formularios, generación de páginas con contenidos dinámicos, etc.), presenta las siguientes características:

- Soporte a múltiples sistemas operativos como, Unix, Microsoft Windows, Mac OS, IBM OS, etc.
- Soporte a múltiples servidores Web: Apache, Microsoft IIS, Netscape, etc.
- Soporte a más de 25 gestores de bases de datos: MySQL, Oracle, dBase, FrontBase, Sybase, Informix, etc.
- Generación de resultados en múltiples formatos como XHTML, XML, imágenes, archivos PDF, películas Flash, etc.
- Funciones de comercio electrónico como Cybercash, CyberMUT, VeriSign Payflow y CCVS para las pasarelas de pago.

Y muchas más posibilidades que siguen aumentando día a día.

6.4 SGBD, Administrador de Bases de Datos MySQL.

Los SGBD o Sistemas Gestores de Bases de Datos, son aplicaciones que permiten al usuario definir, crear y mantener las bases de datos tanto por interfaz de consola como gráfica, dependiendo del sistema que se esté utilizando, proporcionando un acceso controlado a la base de datos.

Los objetivos a cumplir por un SGBD son los siguientes:

- Definir una base de datos mediante un lenguaje de definición de datos, que permita especificar la estructura, tipo de datos y la restricción de los mismos, almacenando todo en la base de datos.
- La misma estructura de la base de datos, debe permitir la inserción, modificación y eliminación de los datos, así como consultas de estos.
- Proporcionar seguridad y acceso controlado a la base de datos, desde el usuario, los datos, el control de recurrencia en uso compartido de datos, control de recuperación en casos de fallas y un diccionario o catálogo de datos accesible a los usuarios.
- Proveer interfaces permitiendo la manipulación por usuarios y programadores.
- Permitir una fácil administración de los datos.

Los SGBD proveen facilidades para la manipulación de grandes volúmenes de datos, simplificando la programación, con un buen manejo de políticas de respaldo se garantiza la consistencia en los cambios de la base de datos, reduciendo los tiempos de desarrollo y aumentando la calidad del sistema desarrollado.

MySQL

MySQL (Structure Querry Language o Lenguaje de Consulta Estructurado), es un SGBD relacionales que usa el modelo cliente / servidor, ofrece compatibilidad principalmente con PHP, Perl, C y HTML, así como de funciones avanzadas de administración y optimización de bases de datos. Implementa funcionalidades Web, lo que permite un accesos seguro y sencillo a los datos a través de Internet.

Su coste es mínimo, incluye un servidor, programas cliente para acceder al servidor, herramientas administrativas y una interfaz de programación para escribir programas. Es portable lo que indica que

se ejecuta en diversos sistemas operativos como Unís, Microsoft Windows, Mac OS, etc.

En la mayoría de las veces se instala el servidor en la computadora que a la vez funcionara como cliente, pero en el caso de que el servidor se encuentra en una computadora y el cliente en otra, será necesario instalar el software cliente en las maquinas cliente para poder conectarse al servidor.

MySQL es software de código abierto escrito en una mezcla de los lenguajes C y C++, es decir, que es posible para cualquier usuario poderlo modificar, cualquier interesado puede descargar el código fuente para estudiarlo y ajustarlo a sus necesidades, pero con algunas restricciones dictadas por la GNU (General Public License).

6.5 Software para trabajo en grupo WorkGroup. Características.

El software para trabajo en grupo también conocido como GroupWare, es el conjunto de hardware y herramientas de software que soportan el trabajo en colaboración de equipos de personas, permitiendo las siguientes características:

- Actividades colaborativas, donde un conjunto de usuarios trabajan en un mismo repositorio de datos para la obtención de resultados en común.
- Actividades cooperativas, aquí los usuarios trabajan sobre su propio conjunto particular estableciendo los mecanismos de cooperación entre ellos.
- Actividades de coordinación, presentando enlaces coherentes entre las actividades y las personas involucradas.

Se trata de herramientas informáticas diseñadas con el propósito de ayudar a los usuarios a trabajar en colaboración de la forma más eficaz, incentivando el flujo de trabajo. Las funcionalidades básicas de las herramientas de software para trabajo en grupo son:

- Comunicación: ayuda a los miembros del equipo al intercambio de información para el cumplimiento de las tareas.
- Coordinación: con mecanismos para el ajuste del desarrollo de las tareas y funciones de los miembros y de las diferentes fases para su control.

- Colaboración: herramientas para el trabajo colaborativo y cooperativo sobre contenidos informativos, tanto estructurados como no estructurados.

Debiendo con esto otorgar servicios tales como, comunicación entre miembros del grupo, compartición de información, coordinación y control de objetos y espacio compartidos y organización del proceso de trabajo, ayudando a la toma de decisiones.

Suele asociarse la aparición y auge de este tipo de software a la herramienta Lotus Notes en la década de 1980, que después fue adquirida por IBM. Ofrecía prestaciones de comunicación, coordinación y trabajo compartido. Hoy en día se destaca la consolidación de herramientas WorkGroup con licencias de software libre, que permite a todo tipo de organizaciones implementar este tipo de actividades en sus entornos. La mayoría de estas herramientas ofrecen un esquema similar basado en un servidor central, conteniendo la información y clientes Web para los usuarios individuales.

Existen diversos tipos de herramientas de trabajo en grupo, pero en realidad lo que define a una herramienta es el uso que se le da, además de las prestaciones que ofrece. Se da una clasificación general según el objetivo principal para el que se usan las herramientas:

- GroupWare del individuo: dedicado a gestionar el trabajo de cada individuo en el grupo.
- GroupWare de documento: se dedica gestionar el ciclo de vida y las tareas sobre un documento.
- GroupWare de proceso: gestiona la ejecución y cumplimiento de fases y tareas.

Todo esto con el fin de que se puedan cumplir diversos objetivos de diferentes formas, con servicios que van desde aplicaciones de mensajería instantánea, correo electrónico, conferencias electrónicas, gestión de colecciones de documentos y proyectos, y más, que colabore con la mejor toma de decisiones para el grupo de trabajo. Dos ejemplos de software dedicado al WorkGroup en el mercado actual han sido desarrollados por, Novell con su Open WorkGroup Suite y otro seria desarrollado por SolidWorks con su PDMWorks Workgroup.

CAPÍTULO 7

Análisis, diseño y programación del sistema propuesto.

7.1 Análisis del sistema.

Una vez que se han revisado y comprendido cada una de las metodologías propuestas por autores dedicados a los temas que envuelven este trabajo de tesis, se procede a tomar las mejores consideraciones en cuanto a que metodología o que aspectos son los más adecuados para que se logren realizar los objetivos establecidos para este trabajo.

Además fueron contempladas y consultadas otras fuentes de información, como lo son; sitios Web de distintas universidades y organizaciones dedicadas a la propuesta y realización de Auditorías en distintos campos y que por su amplio conocimiento han abarcado la Auditoría en Informática. También fue consultado un trabajo de tesis previo realizado en la misma facultad, que propone una integración de diversos elementos dispuestos para la agilización y mejoramiento de la eficiencia y calidad al momento de realizar un trabajo de Auditoría en esta área.

También se contó con la experiencia y conocimiento del asesor de esta tesis, en cuanto a la realización de sistemas de información en todos sus requisitos de fabricación, desde planeación y diagramación, hasta el diseño y programación del mismo sistema.

Es por eso que se logró integrar una serie de módulos prácticos y fáciles de comprender, con un flujo de información basado en las distintas metodologías consultadas, herramientas, requisitos y condiciones, que permitan la obtención de resultados más eficientes, verídicos, rápidos y fáciles de manipular, lo cual llevara a una mejor y más rápida toma de decisiones.

El sistema consta de menús principales, pruebas, formatos, una base de datos acorde a las necesidades del sistema, controles de acceso, registros, consultas, y la documentación necesaria para tener un buen manejo del mismo.

La base de datos consta de la suficiente y necesaria cantidad de tablas y campos para que los usuarios puedan realizar una auditoría de forma más eficiente, cómoda y con resultados más amplios que llevaran a la obtención de información más práctica, veraz y completa para la toma de decisiones.

Las herramientas a usar en la fabricación del sistema, son de libre distribución, desde el SO, pasando por el SGBD y la programación del mismo. Son herramientas confiables, estables y con el soporte y reconocimiento necesarios para los estándares correspondientes y que presentan la estabilidad suficiente para la fabricación del sistema, como el SO Linux Mandriva y Ubuntu, que trabajan con las condiciones óptimas para ofrecer una plataforma estable para las herramientas de programación necesarias. El servidor Web Apache 2, el SGBD MySQL, lenguajes de marcado HTML, XML, XHTML, PHP, son los empleados en este trabajo para la fabricación del sistema.

Todo esto con la finalidad de poder realizar de la manera más sencilla pero segura un sistema capaz de ofrecer calidad, eficiencia, resultados más certeros y confiabilidad a la hora de la toma de decisiones, además de cubrir las necesidades de un mejor control y mantenimiento en el área de Informática de cualquier organización.

7.2 Diseño del sistema

Para el diseño del sistema se emplearon técnicas aprendidas en el transcurso de las distintas materias vistas en la licenciatura, también se usaron herramientas que facilitaron la planeación, diagramación, estructuración y programación del mismo, como los son; software DIA para la realización de diagramas de flujo, software WorkBench de la firma MySQL para la estructuración y diseño de bases de datos, diagramas de entidad y relación en bases de datos, software de texto sencillo para la codificación y formato del sistema en general.

En el anexo de diagramas se muestran como fueron diseñados los flujos de información, así como el control que permite un manejo del sistema más seguro, confiable y efectivo. También contienen, pantallas impresas del producto en algunos puntos más importantes.

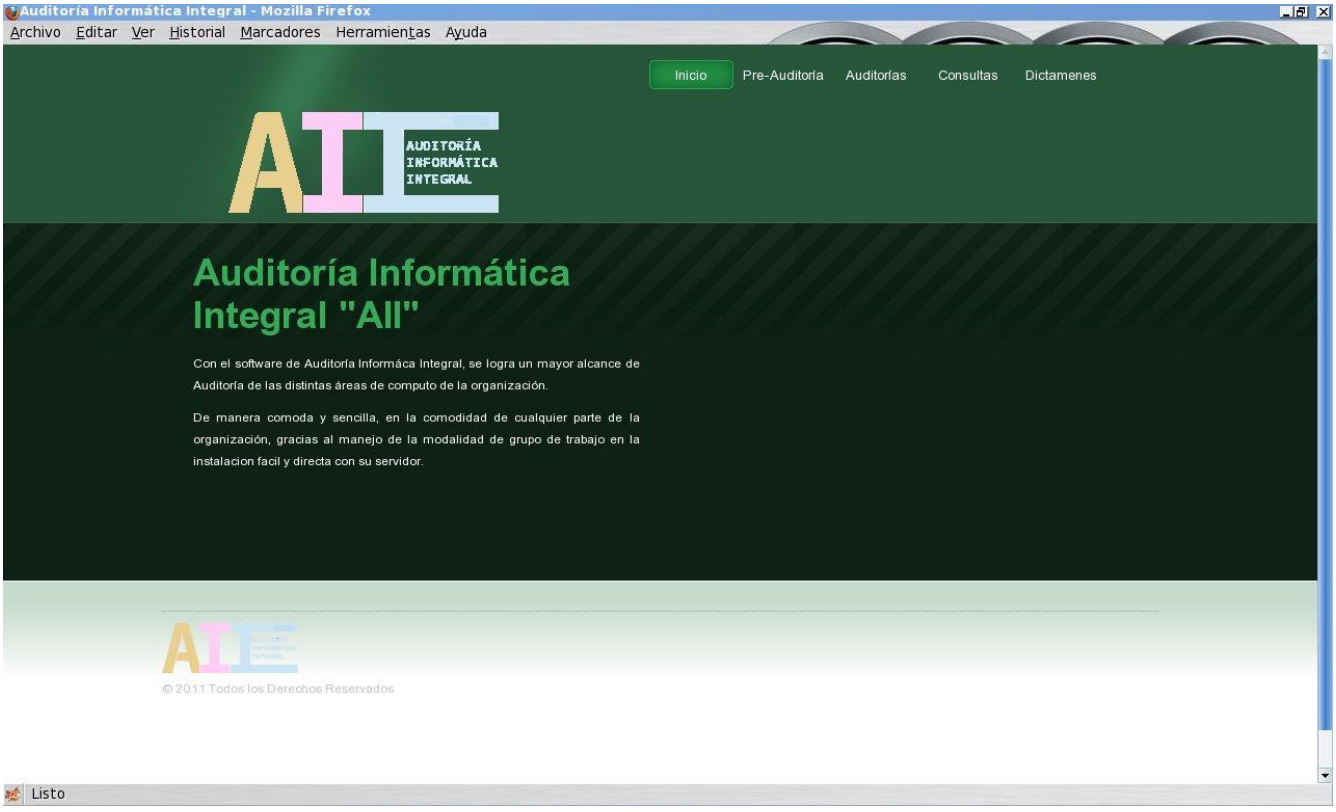
Para la documentación de la información obtenida, desde una pre-auditoría, pasando por el contrato, consultas, la Auditoría misma, el dictamen y la administración del sistema se maneja la herramienta de distribución libre llamada FPDF, que permiten una interfaz con el usuario más fácil de entender y manejar al momento de cualquier impresión de reportes o consultas. Dando un ambiente familiarizado como con cualquier página Web, gracias a las herramientas que se utilizan dando una interfaz de este tipo.

A la vez, el diseño fue basado en las características que envuelven a la Ingeniería de Software, desde métodos a seguir y sus cualidades, hasta contemplar los modelos que maneja para el control de tiempos y actividades al momento de la fabricación de un producto de software.

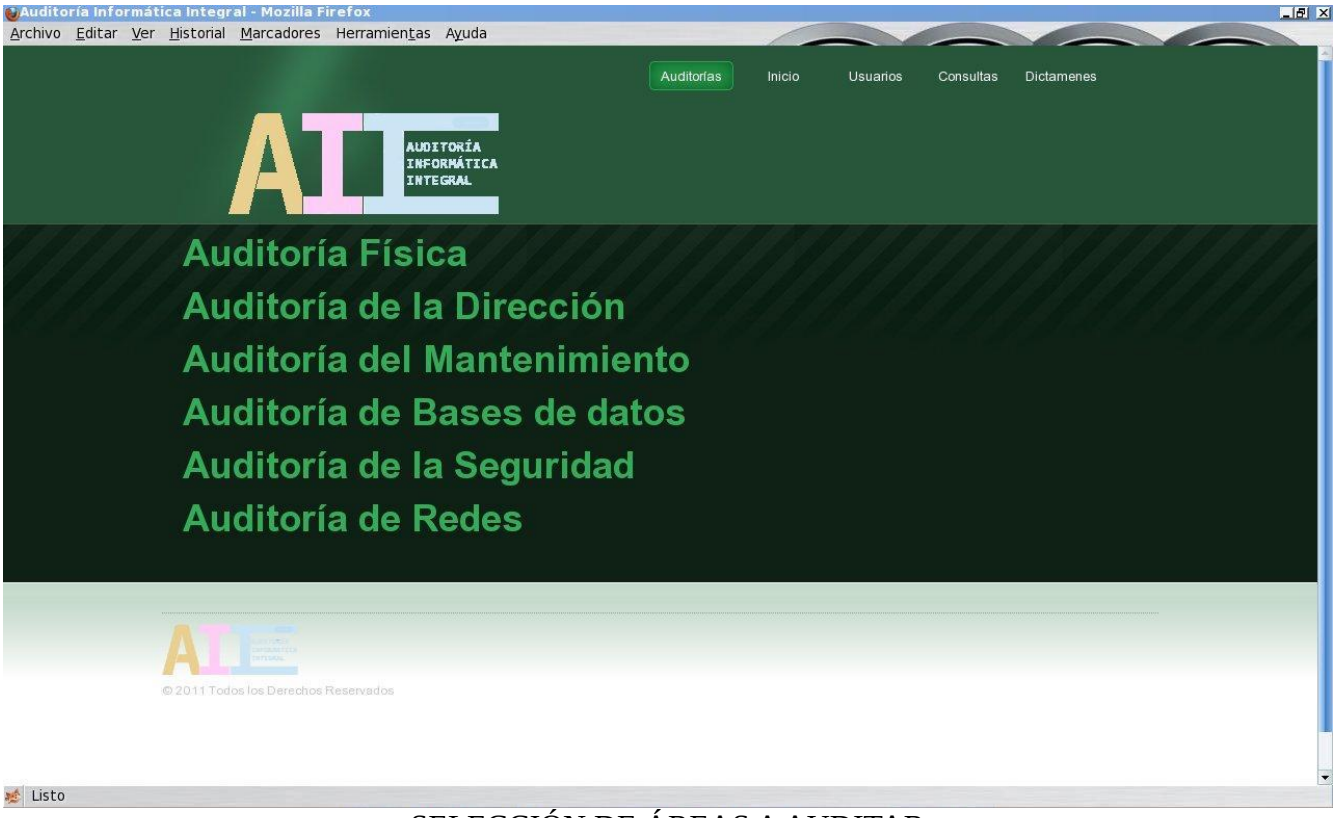
Con la tarea de cubrir métodos y requerimientos necesarios en la creación de un sistema, se hizo la investigación necesaria para la selección de cada una de las herramientas que se utilizan en este caso, para dar un ejemplo claro de que se tiene suficiente información como para hacer de la Auditoria en Informática una práctica esencial en toda organización, para un mejor rendimiento y rentabilidad de la misma. Todas y cada una de las herramientas utilizadas son de fácil manejo, acceso e instalación en todo SO.

7.3 Programación del sistema

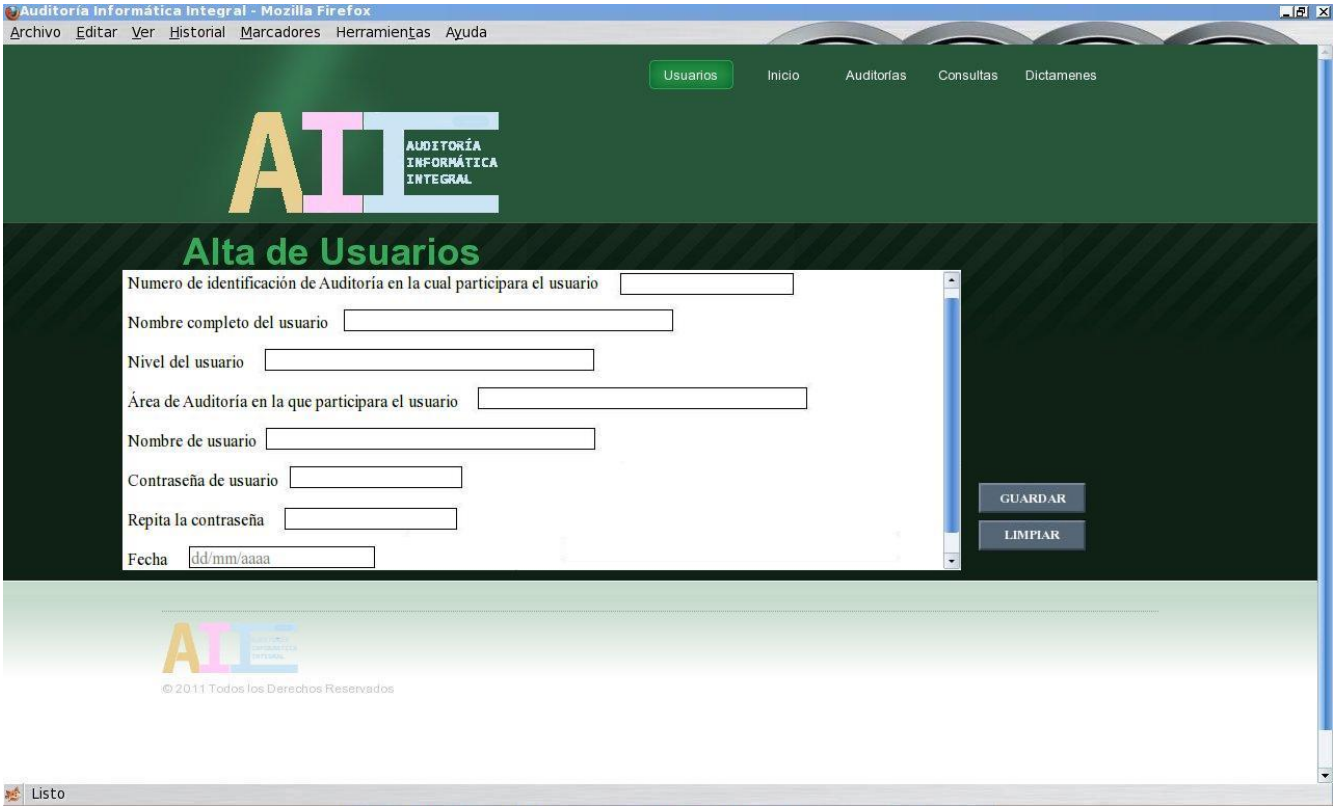
Aquí se mostraran impresiones de pantallas como ejemplos algunas de las partes más importantes del sistema realizado en este trabajo, el cual fue nombra como Auditoría Informática Integral AII.



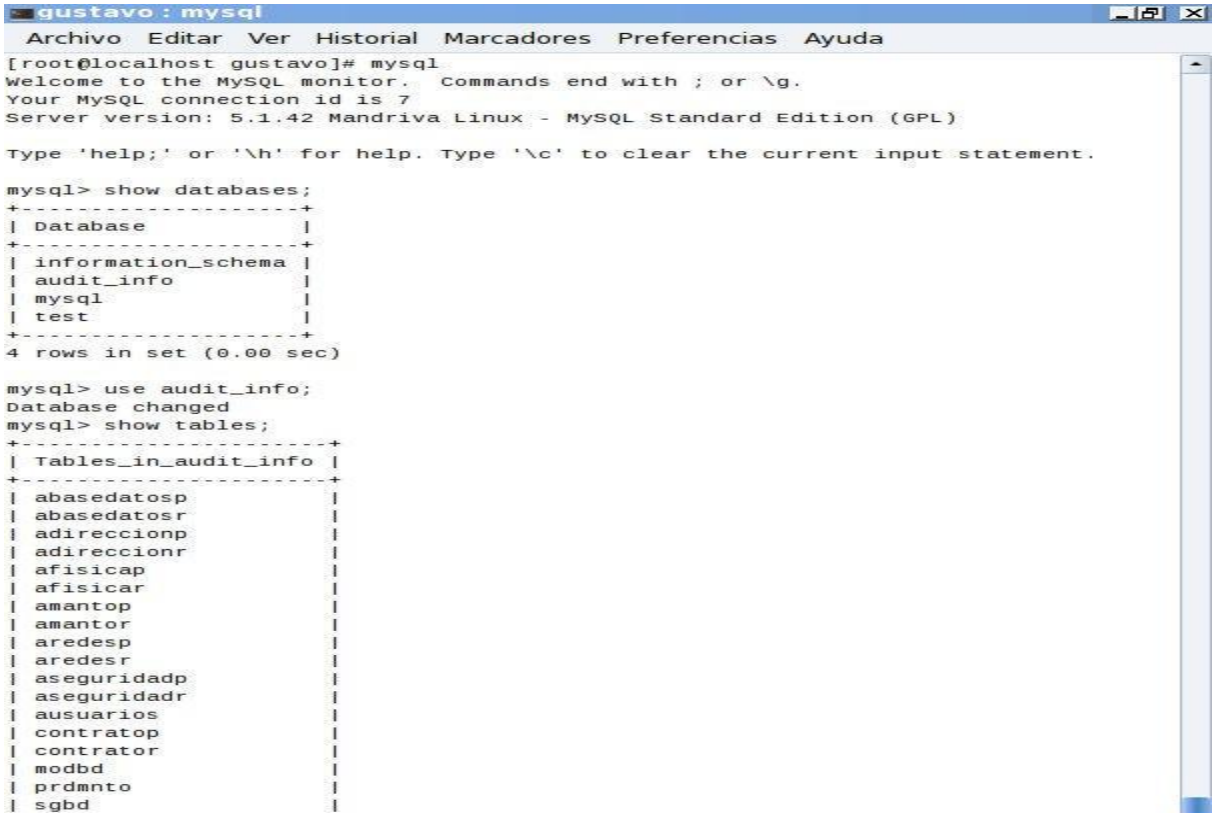
PAGINA DE INICIO



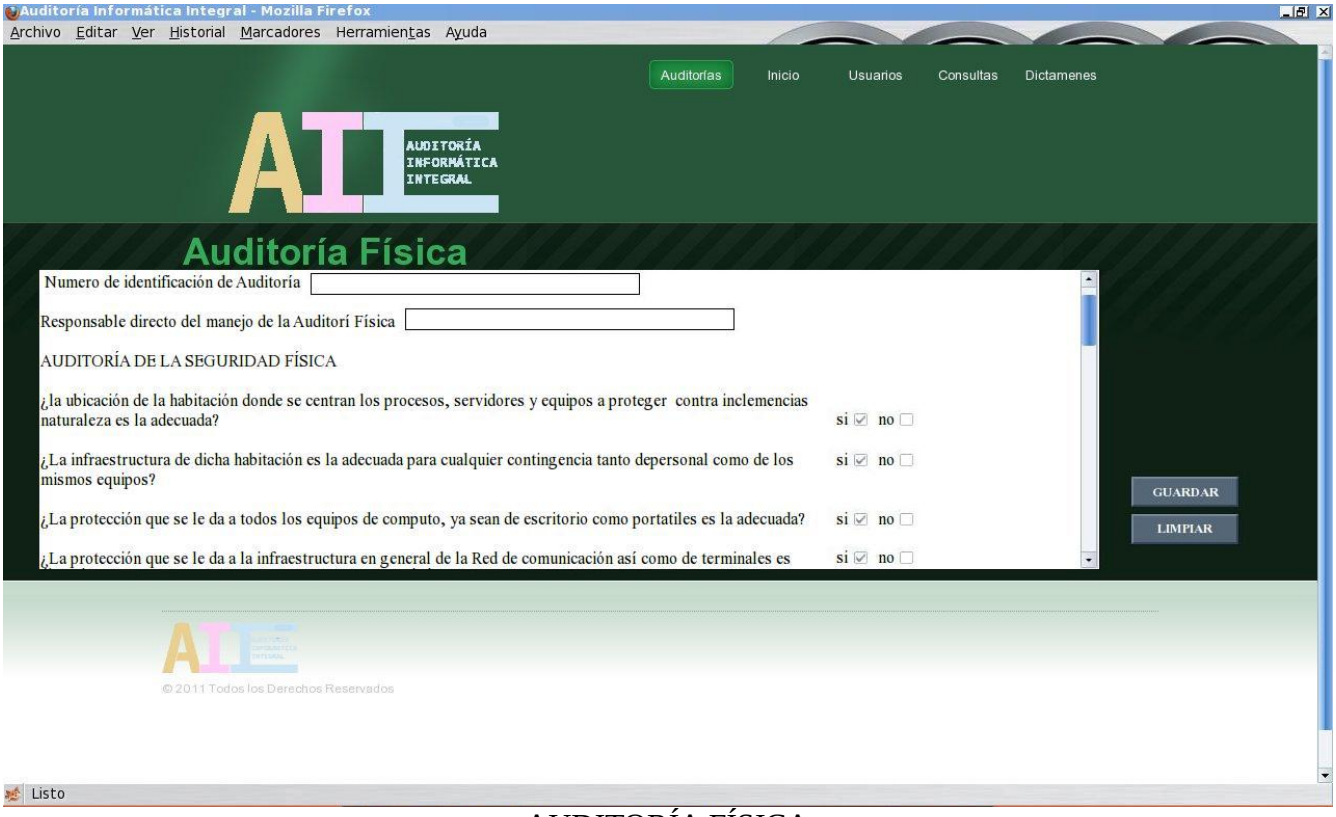
SELECCIÓN DE ÁREAS A AUDITAR



ALTA DE USUARIOS



BASE DE DATOS PRINCIPAL CON ALGUNAS DE LAS TABLAS DE LA MISMA



AUDITORÍA FÍSICA

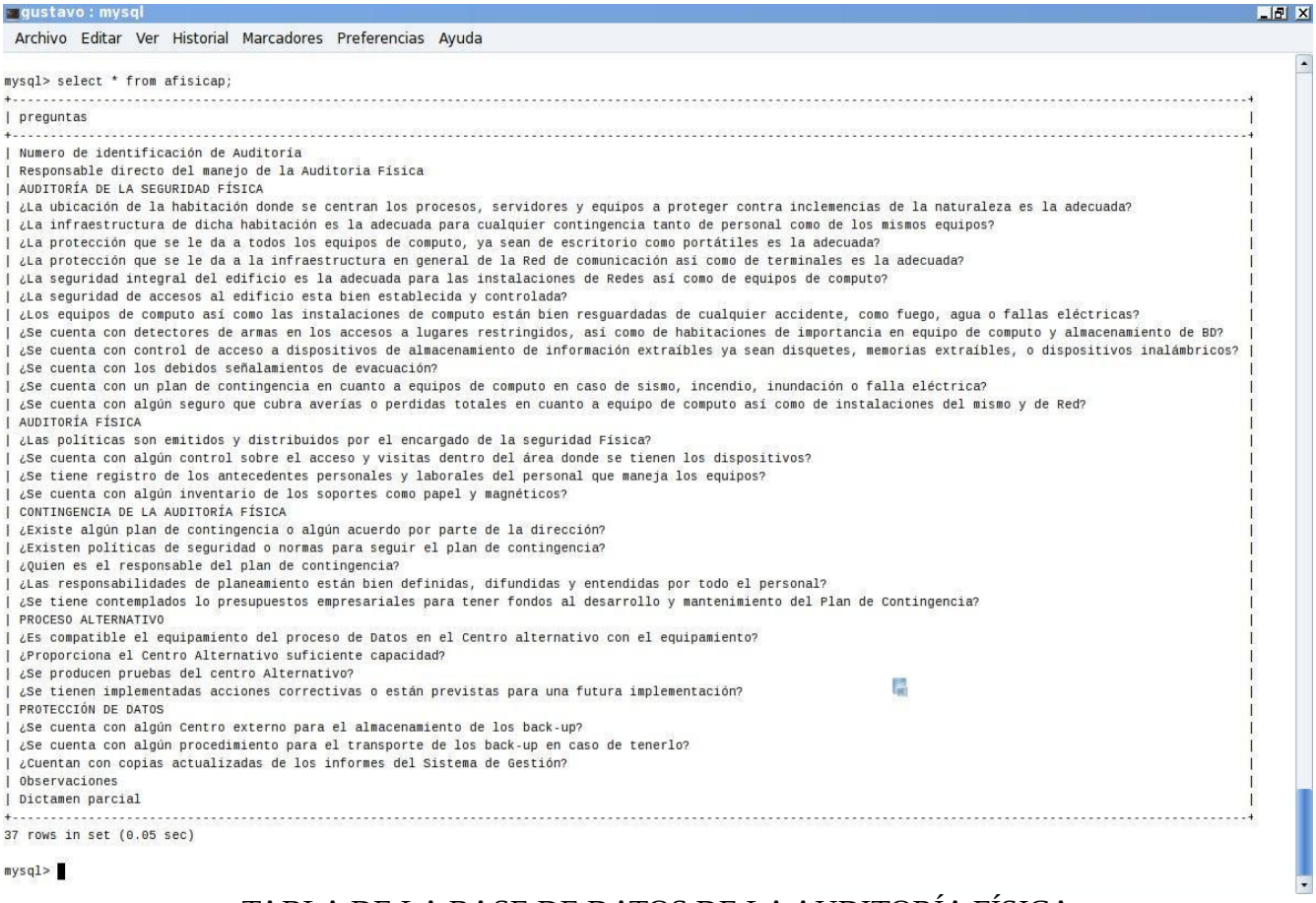
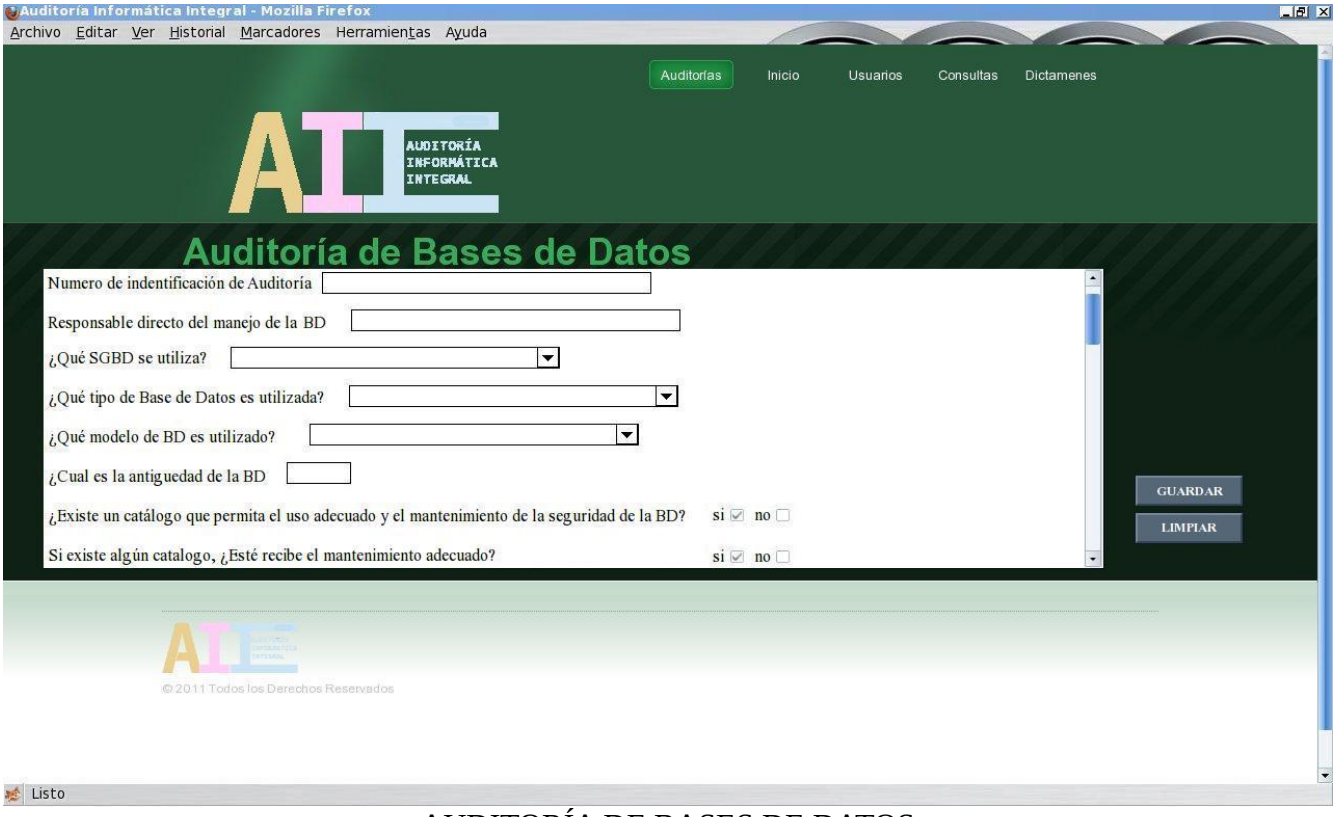


TABLA DE LA BASE DE DATOS DE LA AUDITORÍA FÍSICA



AUDITORÍA DE BASES DE DATOS

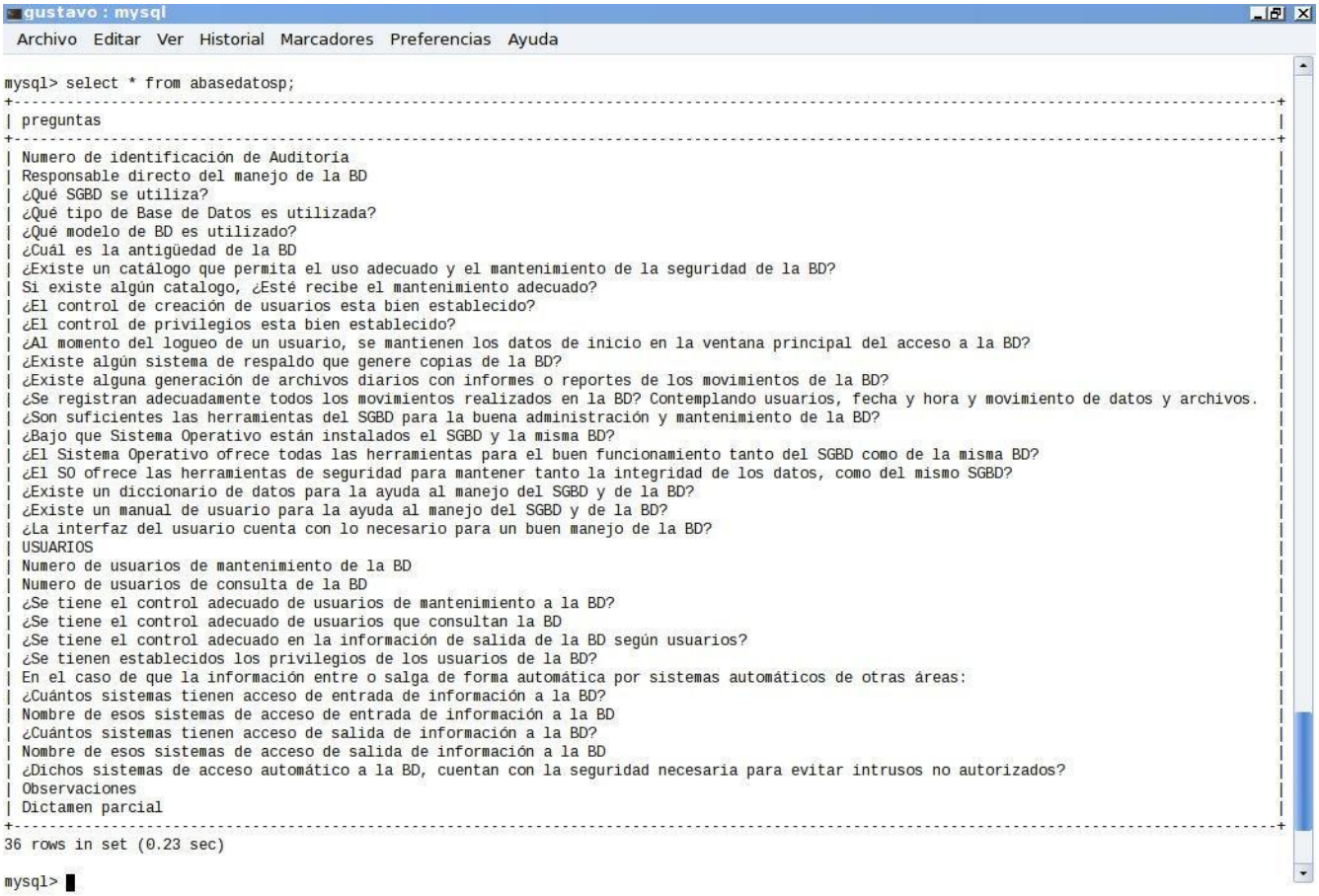


TABLA DE LA BASE DE DATOS DE LA AUDITORÍA DE BASES DE DATOS

AUDITORÍA DE REDES

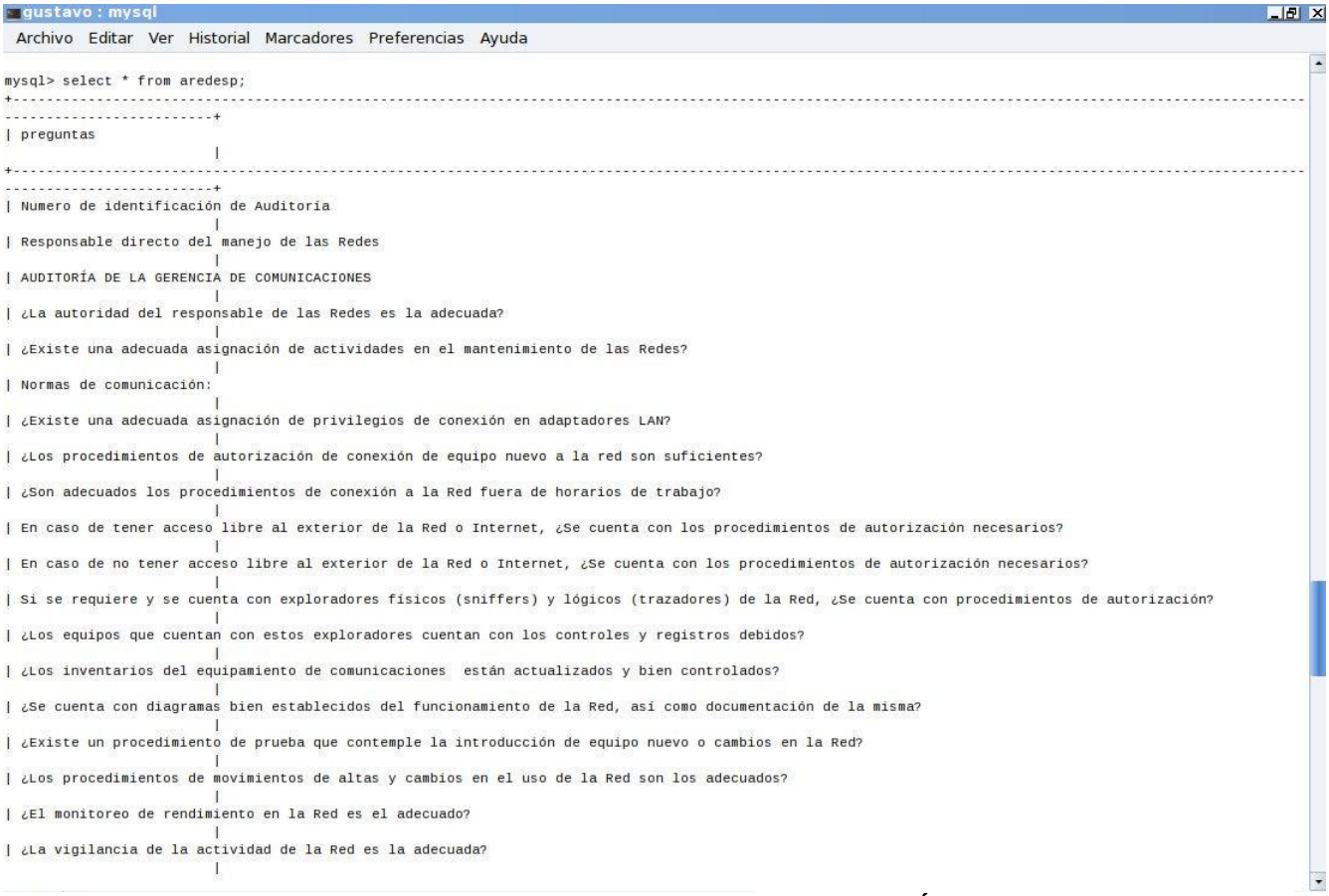


TABLA DE LA BASE DE DATOS DE LA AUDITORÍA DE REDES

CONCLUSIONES

CONCLUSIONES

Los centros de cómputo antes no eran planeados para una organización, es más, no eran tomados en cuenta con alguna importancia, en la actualidad han ido creciendo y su distribución ha cambiado logrando una descentralización, esto hace que su administración sea cada vez más compleja en áreas críticas y que requiera de evaluaciones periódicas, formales e imparciales, pera ello un apoyo exterior con una metodología eficiente ayuda a controlar los centros de cómputo.

Las herramientas específicas definidas en esta propuesta de metodología son utilizadas para lograr que la empresa sea administrada y dirigida eficientemente en el ámbito de las tecnologías de información.

El uso de las tecnologías de información facilita la auditoría en Informática ya que a lo largo del tiempo han ido desarrollándose con el objetivo de utilizarlas para maximizar sus beneficios y así proyectarlo en la actividad que se realice.

Al llevar a cabo una auditoría en Informática los directivos sabrán si se está administrando y dirigiendo de manera correcta todos los recursos informáticos contando con un proceso de auditoría en informática digerible, práctico y eficiente que facilite tanto el planeamiento oportuno de las recomendaciones, como los cursos de acción requeridos para una solución integral. De esta manera, la auditoría en Informática se convierte en un impulsor de las organizaciones para obtener resultados esperados de dicha tecnología en los tiempos, costos, beneficios, calidad y otros factores recomendados para acercarse a ser una organización de alta calidad y competir en terrenos de las tecnologías de información.

Por último, cabe mencionar que con esta propuesta se pretende mejorar y poner en práctica en cada una de las áreas con que la auditoría informática cuenta; los beneficios que se obtienen, dejando abierta la oportunidad de encontrar y mejorar cada una de las fases en cada área de la auditoría informática.

Con lo anterior, se demuestra el hecho de que los objetivos planteados fueron logrados, ya que las herramientas usadas, así como la metodología, abarcan una Auditoría Informática en las principales áreas de Informática de cualquier organización, instalado y probado en el servidor principal, y funcionando con la modalidad WorkGroup antes planteada.

BIBLIOGRAFÍA

- Auditoría en Informática ``Un enfoque metodológico y práctico". Enrique Hernández Hernández. Ed. CECSA. México, 1995.
- Auditoría en Informática. José Antonio Echenique García. Ed. Mc Graw Hill, México, 2002.
- Auditoría en Informática. Un enfoque práctico. Mario Piattini Velthuis y Emilio del Peso. Ed. Alfaomega, Ra-Ma. México.
- Técnicas de la Auditoría en Informática. Yan Derrien. Ed. Alfaomega, marcombo, México, 1995.
- Beginning XML. David Hunter. Ed. wrox programer to programer, USA, 2000.
- The complete reference MySql. Vikram Vaswani. Ed. Mc Graw Hill Osborne, USA, 2004.
- Diseño conceptual de bases de datos, un enfoque de entidades - interrelaciones. Batini Ceri Navathe. Ed. Addison-Wesley/Diaz de Santos. USA, 1994.
- Ingeniería de Software. Richard Fairley. Ed. Mc Graw Hill. México, 1987.
- Publicar con HTML en internet. Heslop and Budnick. Ed. Thomson editores. España, 1996.
- Creación de un portal con PHP y MySql. Jacobo Pavón Puertas. Ed. Alfaomega Ra-Ma. México, 2007.
- Beginning Web programming with HTML, XHTML, and CSS. Jon Duckett. Ed. Wiley. USA, 2004.

ANEXO

DIAGRAMAS DE FLUJO DEL SISTEMA

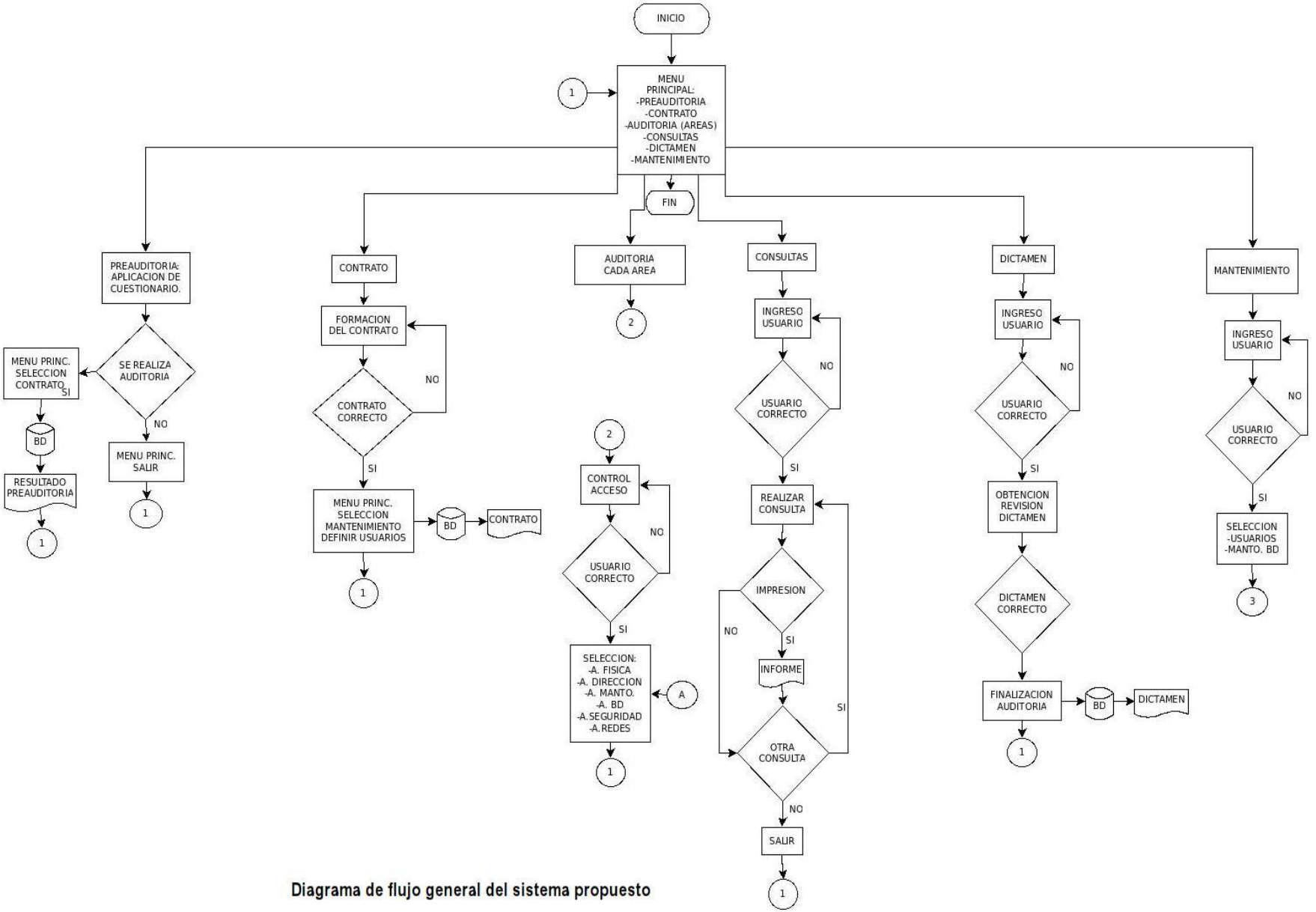
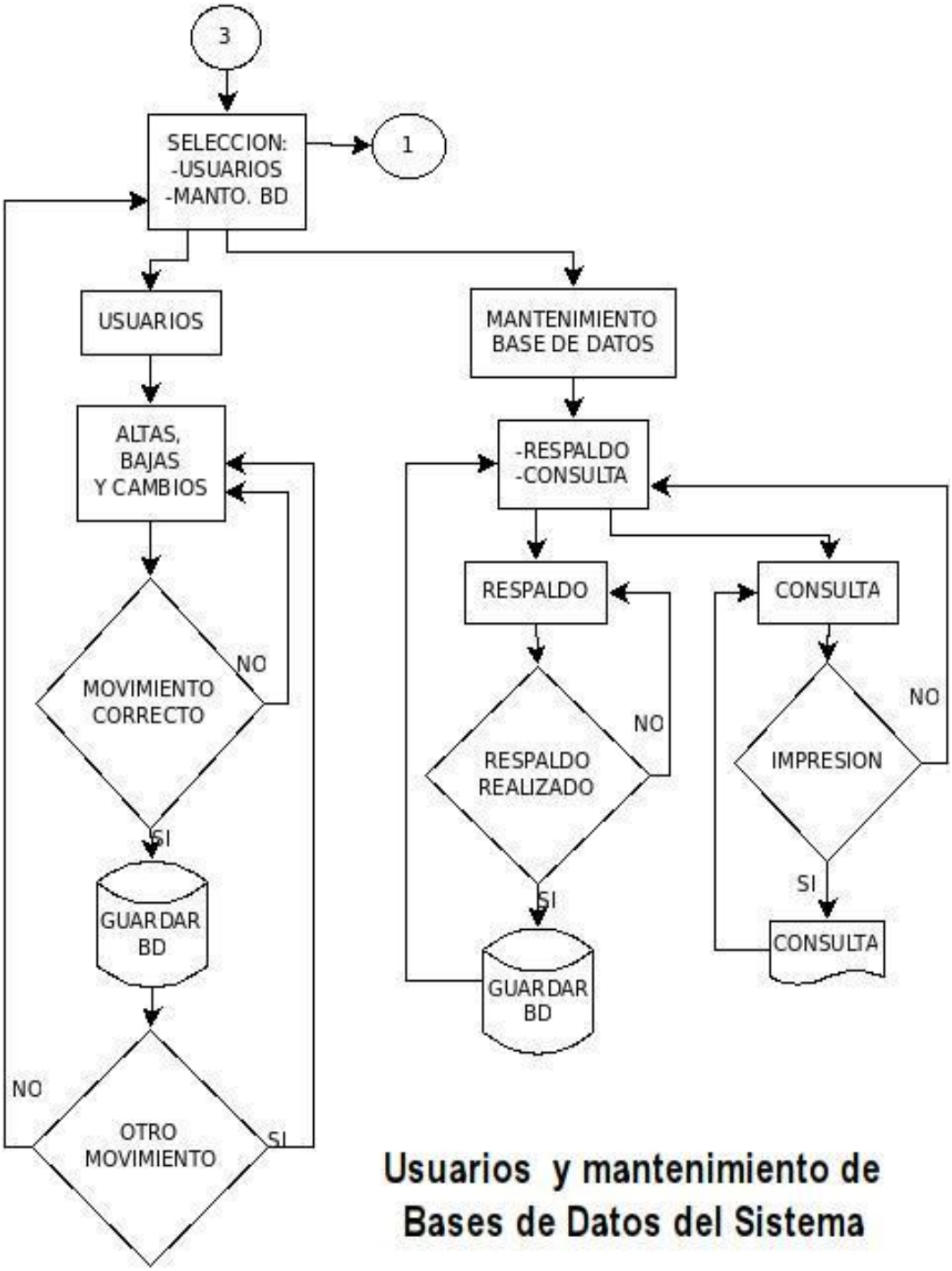
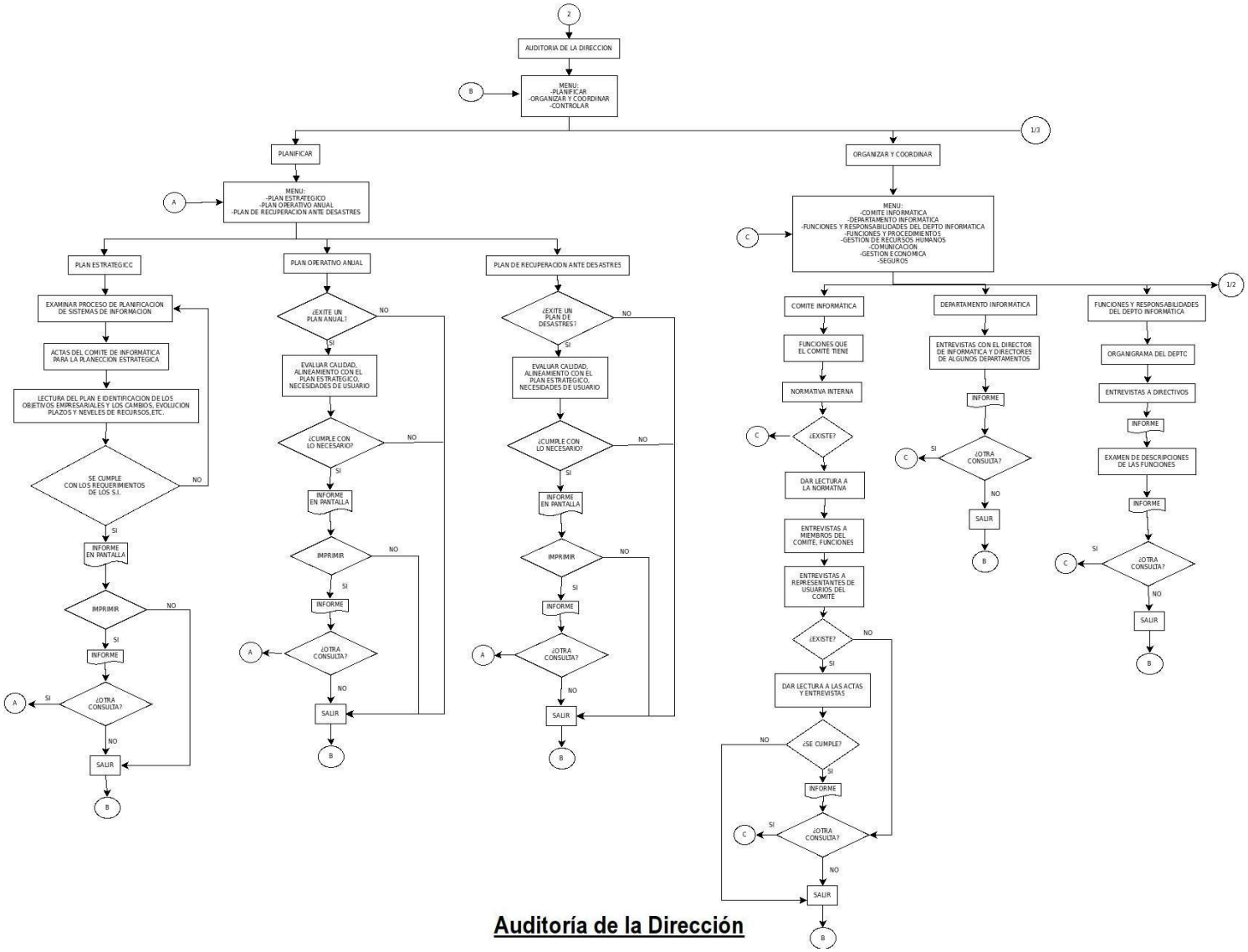


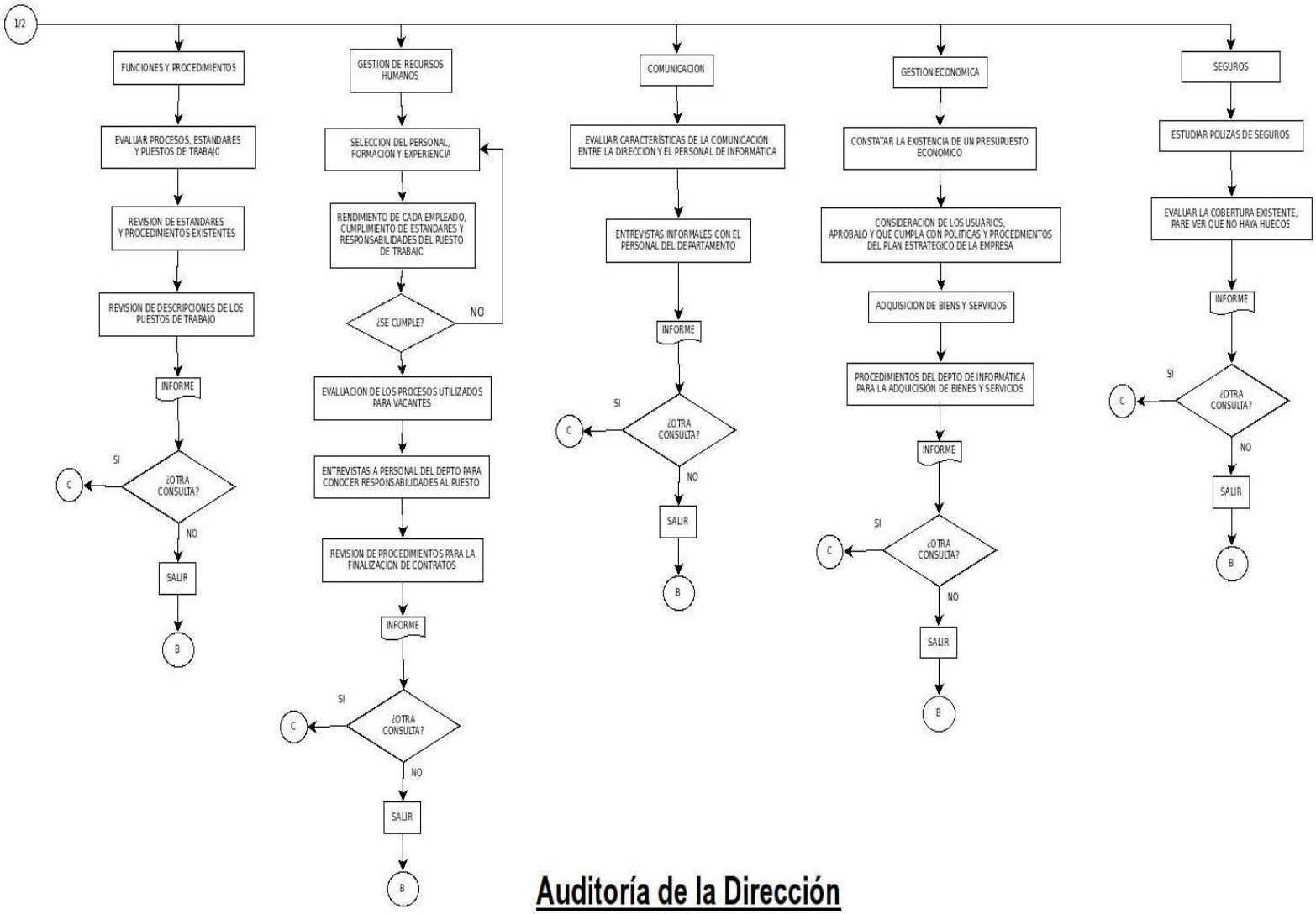
Diagrama de flujo general del sistema propuesto



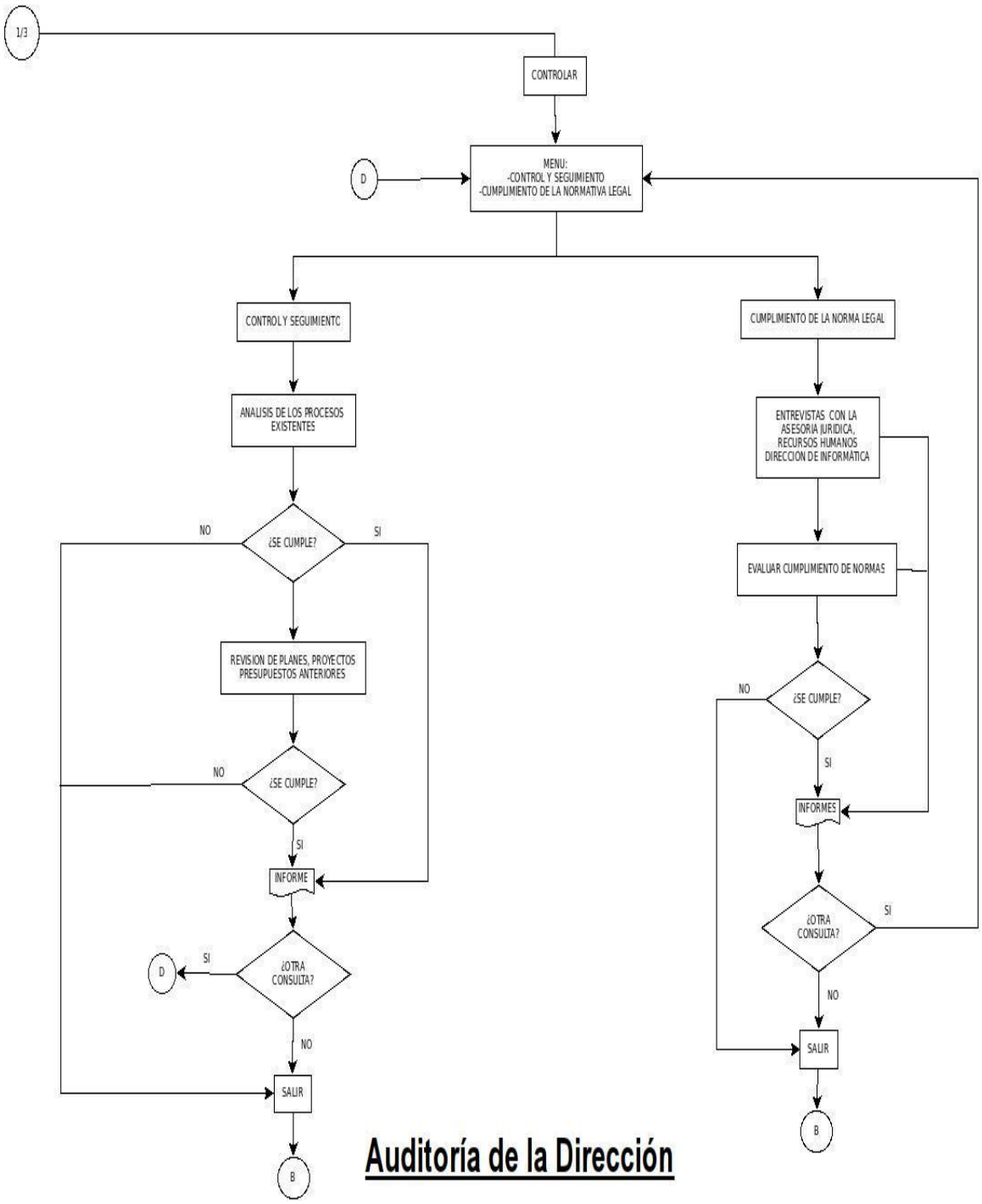
Usuarios y mantenimiento de Bases de Datos del Sistema



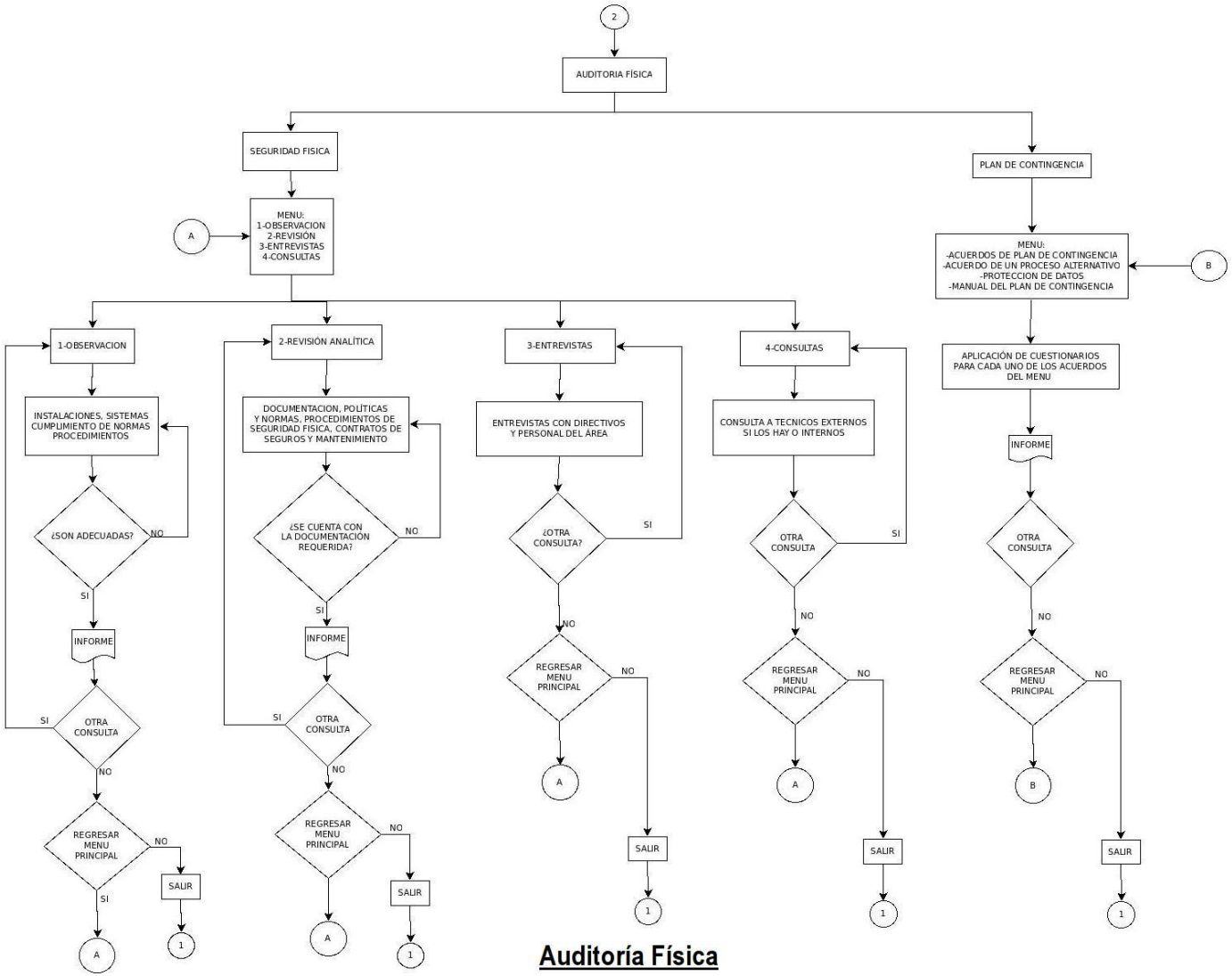
Auditoría de la Dirección



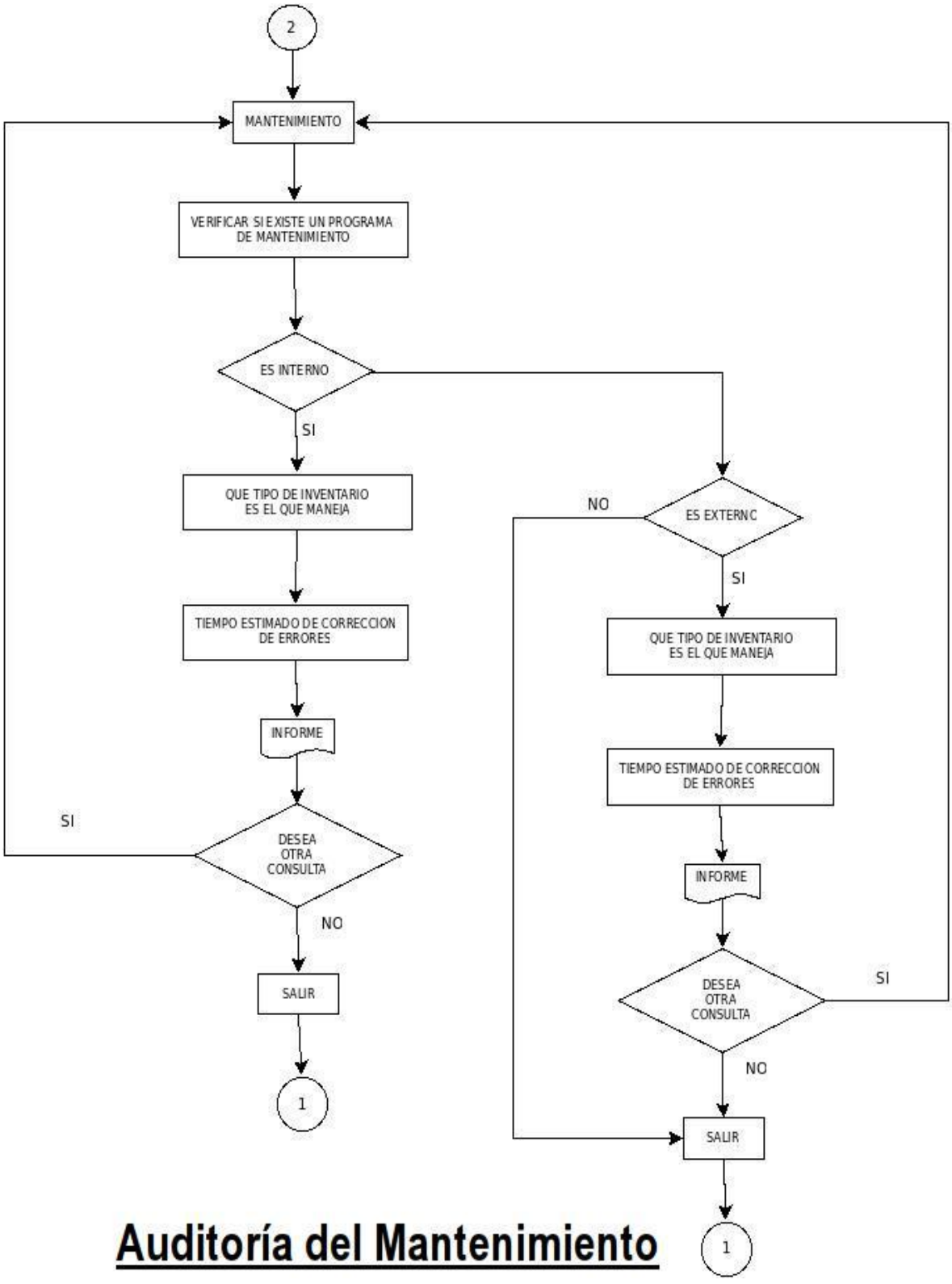
Auditoría de la Dirección



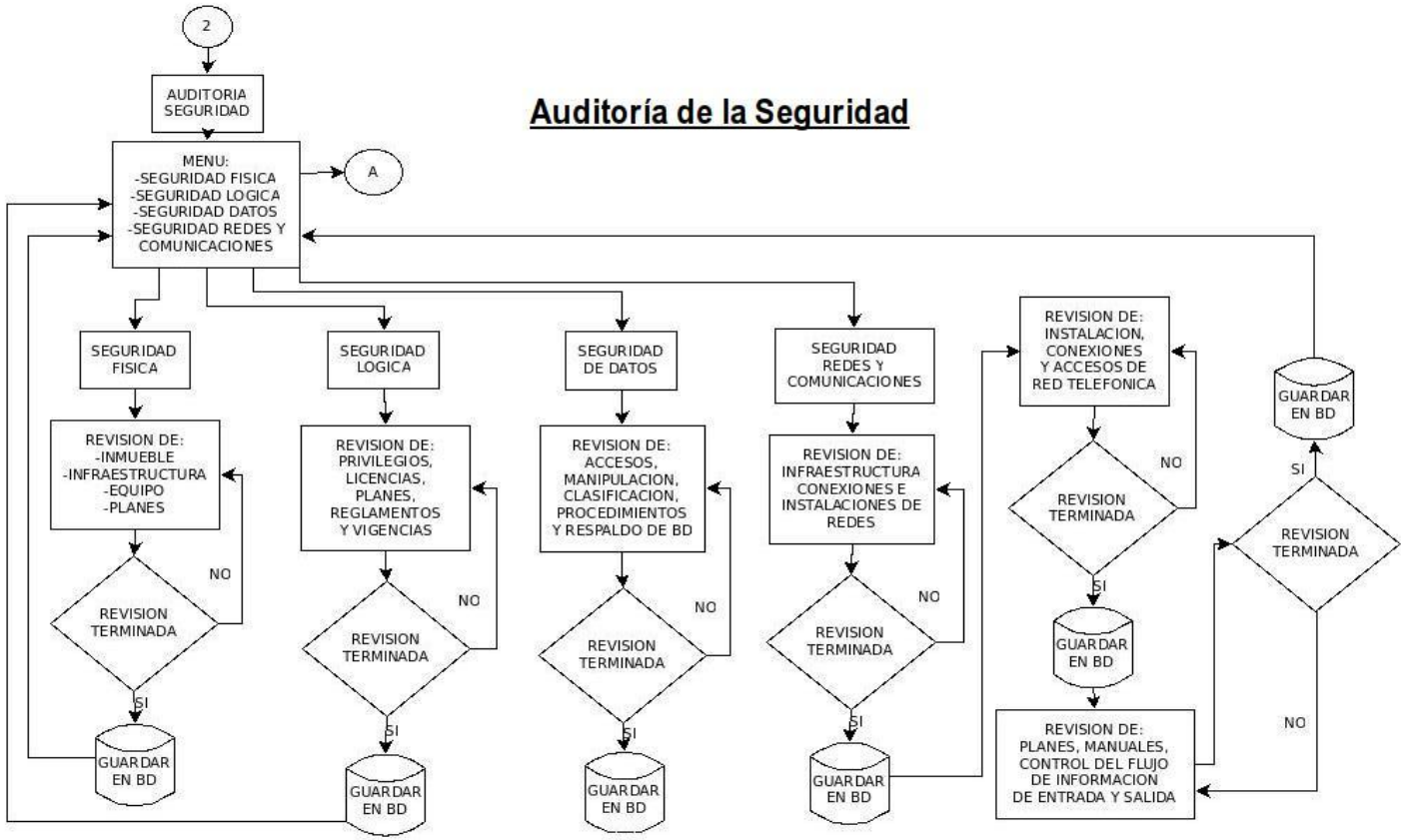
Auditoría de la Dirección

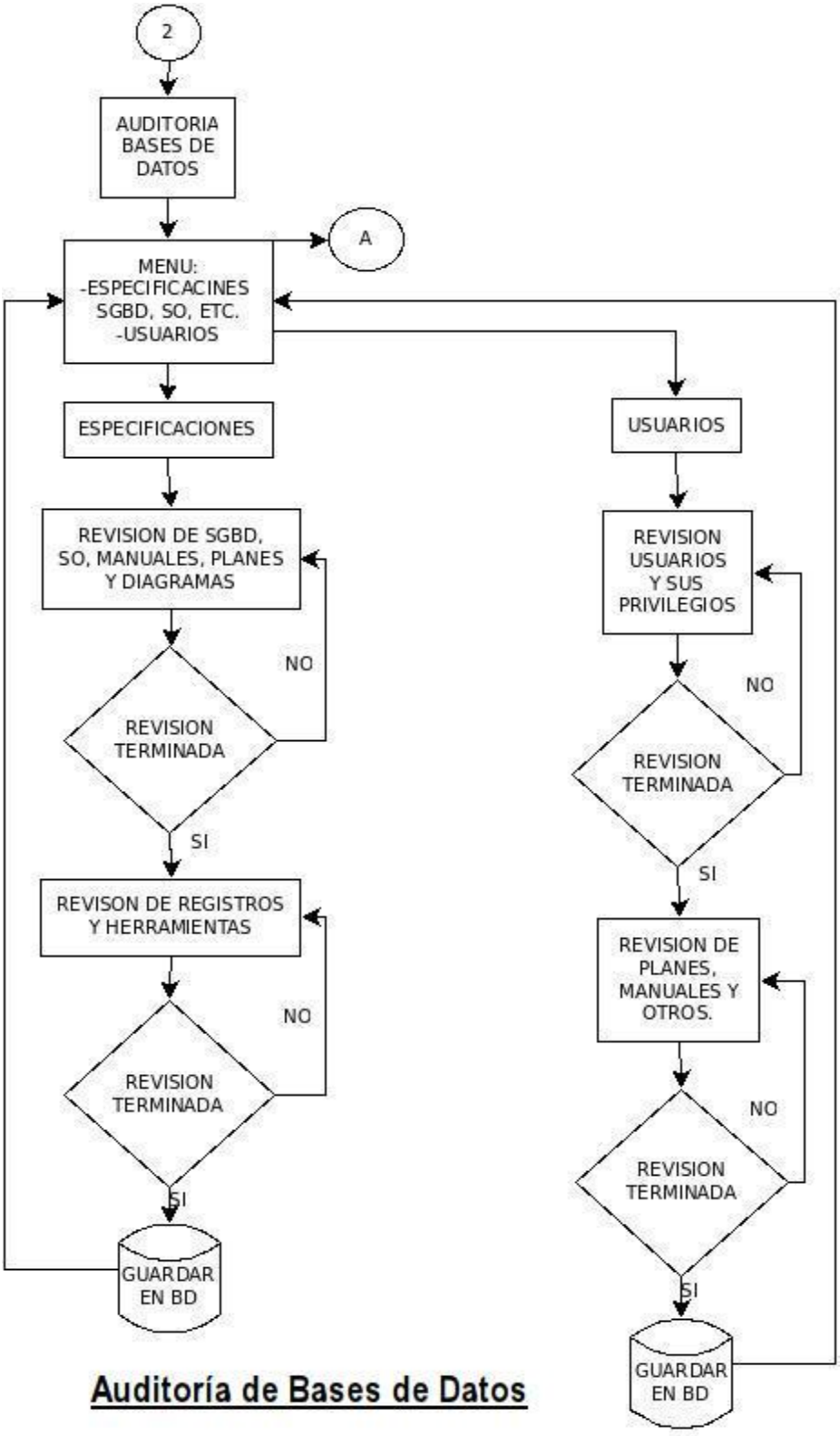


Auditoría Física



Auditoría del Mantenimiento


2
AUDITORIA SEGURIDAD
Auditoría de la Seguridad
MENU:
-SEGURIDAD FISICA
-SEGURIDAD LOGICA
-SEGURIDAD DATOS
-SEGURIDAD REDES Y COMUNICACIONES
A
SEGURIDAD FISICA
SEGURIDAD LOGICA
SEGURIDAD DE DATOS
SEGURIDAD REDES Y COMUNICACIONES
REVISION DE: -INMUEBLE -INFRAESTRUCTURA -EQUIPO -PLANES
REVISION DE: PRIVILEGIOS, LICENCIAS, PLANES, REGLAMENTOS Y VIGENCIAS
REVISION DE: ACCESOS, MANIPULACION, CLASIFICACION, PROCEDIMIENTOS Y RESPALDO DE BD
REVISION DE: INFRAESTRUCTURA CONEXIONES E INSTALACIONES DE REDES
REVISION DE: INSTALACION, CONEXIONES Y ACCESOS DE RED TELEFONICA
REVISION DE: PLANES, MANUALES, CONTROL DEL FLUJO DE INFORMACION DE ENTRADA Y SALIDA
REVISION TERMINADA
NO
SI
GUARDAR EN BD



Auditoría de Bases de Datos