UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURIA PÚBLICA

"AUDITORÍA APLICADA A UN SISTEMA INFORMATICO INTEGRADO EN DESARROLLO DEL SECTOR MEDICO HOSPITALARIO UBICADO EN LA ZONA METROPOLITANA DE SAN SALVADOR"

Trabajo de Graduación Presentado por:

Alvarenga Ostorga, Yesenia Mercedes

Gómez Rivas, Nydia Aymeé

Yazbek Hernández, Idis Jazmín

Para optar al grado de:
"Licenciado en Contaduría Pública"

Noviembre, 2007

San Salvador, El Salvador, Centro América

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:	Msc. Rufino Antonio Quezada
Secretaria General	:	Lic. Douglas Vladimir Alfaro Chávez

Facultad de ciencias Económicas

Decano	:	Msc. Roger Armando Arias Alvarado
Secretaria	:	Lic. Vilma Yolanda Vásquez de Del Cid
Docente Director	:	Lic. Juan Vicente Alvarado Rodriguez
Coordinador del Seminario	:	Lic. Álvaro Edgardo Calero Rodas

Noviembre de 2007

San Salvador, El Salvador, Centro América

AGRADECIMIENTOS

Gracias Padre Jehová, Señor de Señores, por brindarme perseverancia y sabiduría para alcanzar un éxito mas en la vida, a mis padres, Santos y Blanca y a mi hermana Vicenta por su apoyo incondicional tanto económica como moralmente, a mi esposo Carlos por estar siempre a mi lado ayudándome a seguir adelante en lo académico y en lo personal, por haber sido y por ser el que me sostiene en los momentos mas difíciles de mi vida, a mi pequeño hijo Carlos Salvador por existir y por ser mi mayor incentivo de lucha, a mis amigos y compañeros mis agradecimientos

Yesenia Mercedes Alvarenga Ostorga

Doy gracias primeramente a Dios Todopoderoso, por su misericordia, fortaleza, sabiduría y su fidelidad en cada momento de mi vida y en la culminación de éste trabajo de graduación, doy gracias a mis padres y demás familia, compañeros de trabajo y amigos por el apoyo moral en cada momento de tomar decisiones.

Nydia Aymeé Gómez Rivas

A Dios todo poderoso por ser la luz en mi vida,
A mi madre por ser ejemplo de lucha y perseverancia,
A mi esposo por todo el amor y apoyo brindado,
A toda mi familia, amigos y compañeros que me brindaron apoyo.
Gracias

Idis Jazmín Yazbek Hernández

AGRADECIMIENTOS DEL GRUPO.

Agradecemos a nuestro asesor especialista Lic. Juan Vicente Alvarado Rodríguez por su tiempo, dedicación y esmero. Por colaborar con nuestra formación profesional, por su orientación, comprensión y paciencia durante el proceso del trabajo de graduación.

INDICE

RESUMEN EJECUTIVO

La elaboración de este trabajo de investigación consiste en proponer una aplicación de auditoria a un sistema informático integrado en desarrollo como una herramienta que fortalezca la adecuada toma de decisiones en el área médico/hospitalario de la zona metropolitana de San Salvador.

Para la realización de este trabajo se hizo una investigación documental y de campo; dentro de la investigación documental se obtuvo información sobre las aplicaciones y conocimientos de auditoria en el área de informática en los centros de atención de salud, al respecto se tiene que la red hospitalaria está formada por hospitales privados y entidades autónomas; donde cada uno de estos tiene un breve conocimiento de la aplicación de auditoria en desarrollo.

También incluye el marco teórico conceptual en el cual se fundamenta lo referente a auditoria informática en desarrollo, así también la clasificación y aplicación de

las diferentes normativa técnica contable y legal que le son aplicables.

Dentro de las normas técnicas contables se tiene, la Norma Internacional de Contabilidad número 38, la cual hace referencia a señalar el tratamiento contable de los Activos Intangibles además se incluyeron las Normas Internacionales de auditoria No. 620 uso del trabajo de un experto y las Normas de Auditoria de Sistemas de Información.

Dentro de la normativa legal se incluyeron Ley de Propiedad Intelectual, código Penal, Ley Reguladora del Ejercicio de la Contaduría, Código de Trabajo, Código Tributario, Ley del Impuesto Sobre la Renta, Ley del Impuesto a la Transferencia de Bienes Muebles y a la Prestación de Servicios.

Con respecto a la investigación de campo se aplicó la técnica de la encuesta, utilizando como instrumento el cuestionario y la entrevista, para la obtención de datos que sirvieron para comprender la situación en que se encuentran las unidades de informática de los hospitales

privados y autónomos descentralizados del Gobierno Central, ubicados geográficamente en la zona metropolitana de San Salvador, estos instrumentos de recolección de datos fueron dirigidos a las Jefaturas de Informática de los 8 hospitales objetos de estudio.

Finalmente la tercera fase de la investigación consistió en proponer la aplicación de la planeación de auditoria aun sistema en desarrollo integrado representándolo con un caso ilustrativo el cual fue enfocado en la tercera fase del ciclo de vida de un sistema, se tomo como prueba el sistema SAP que actualmente esta en desarrollo en el Instituto Salvadoreño del Seguro Social, realizando un estudio de la forma lógica como funcionara el sistema y la relación entre los distintos componentes. Dentro de las conclusiones que se obtuvieron con la realización de esta propuesta están:

1. Es fundamental que las instituciones médico/hospitalario apliquen auditoría aun sistema en desarrollo, ya que al aplicarla este permitirá la evaluación y verificación de la información que se

desee que genere y sobre todo esta debe ser confiable y oportuna para la adecuada toma de decisiones.

2. En las instituciones que brindan servicios médico/hospitalario, en las áreas de informática deberán aplicar auditoria a un sistema, porque esta fase es muy importante y trascendental ya que es donde se definen los controles, configuraciones y parametrizaciones del sistema que se implementara; y es donde necesita la evaluación de un auditor para que este verifique si se esta aplicando y cumpliendo según los requerimientos solicitados por la institución.

INTRODUCCIÓN

Con frecuencia, el uso de la tecnología de información para la globalización y la reingeniería de procesos empresariales da como resultado el desarrollo de sistemas de información que ayudan a una empresa a darle ventaja competitiva en el mercado. Es por ello que se ve la necesidad de garantizar la ejecución de esta fase de la mejor manera, es aquí donde la Auditoria Informática sirve de herramienta para lograr este objetivo.

El presente trabajo tiene como finalidad el proponer la planeación de auditoria a un sistema en desarrollo aplicados al área médico/hospitalario, de tal forma que puedan contar una herramienta que permita generar información confiable sobre la aplicación de auditoría informática y contribuya a la toma de decisiones.

Con éste trabajo se ha procurado desarrollar en forma técnica y práctica un memorando de planeación aplicable al ciclo de vida de un sistema en desarrollo aplicable a las instituciones que prestan servicios de salud, por tanto se ha recopilado y analizado información relacionada a la auditoria informática en desarrollo, permitiendo de ésta forma presentar un desarrollo aceptable y aplicable a la realidad en la cual se desenvuelven éste tipo de instituciones.

Para comprender esta temática se plantea los antecedentes, el concepto, las características, los objetivos, la importancia , y los riesgos asociados a la Auditoría Informática, esto de forma general para llegar a comprender la auditoria aplicada al desarrollo de proyectos, su concepto, objetivos, finalidad, ventajas, desventajas y sus etapas, complementándolo con la evaluación del control interno y los riesgos; todo esto contenido en el Capitulo I el cual sirve como un preámbulo para entender la problemática que se desarrolla en el CAPITULO II; en donde se define la metodología empleada , el tipo de investigación y estudio, se determina la muestra, y la unidad de análisis, además se definen las técnicas utilizadas para luego presentar el análisis de datos para poder obtener así el diagnóstico de la investigación.

Una vez constatado el problema se procede a presentar en el Capitulo III la propuesta de solución que consiste en el desarrollo de la planeación de una auditoria informática aplicada a la etapa de desarrollo de un sistema integrado la que contiene la siguiente estructura: Antecedentes de la Institución, objetivos de la auditoria, información sobre el área de sistemas, evaluación del riesgo, alcance de la auditoria, la descripción de la forma de ejecución de trabajo de auditor, incluyendo el presupuesto de recursos, el cronograma de actividades y los procedimientos de auditoría ha aplicar.

Para concluir con el trabajo de investigación sobre esta problemática se presentan las conclusiones y recomendaciones en el Capítulo IV.

CAPITULO I: MARCO TEORICO.

1.1. ANTECEDENTES DE AUDITORÍA.

1.1.1 A nivel mundial.

La importancia de la auditoría es reconocida desde los tiempos más remotos, teniéndose conocimientos de su existencia ya en las lejanas épocas de la civilización sumaria.

Acreditase, todavía, que el termino auditor evidenciando el titulo del que practica esta técnica, apareció a finales del siglo XVIII, en Inglaterra durante el reinado de Eduardo I.

En diversos países de Europa, durante la edad media, muchas eran las asociaciones profesionales, que se encargaban de ejecutar funciones de auditoría, destacándose entre ellas los consejos Londinenses (Inglaterra), en 1310, el Colegio de Contadores, de Venecia (Italia), 1581.

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la ley. Desde 1862 hasta 1905, la profesión de auditoría creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. El hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas.

También en los Estados Unidos de Norteamérica, una importante asociación cuida las normas de auditoría, la cual publicó diversos reglamentos, de los cuales el primero que conocemos data de octubre de 1939, en tanto otros consolidaron las diversas normas en diciembre de 1939, marzo de 1941, junio de 1942 y diciembre de 1943[1].

1.1.2. A nivel nacional.

A finales del siglo XX, los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial.

La informática actualmente, está incorporada en la gestión integral de la empresa; sus normas y estándares propiamente informáticos se encuentran sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa, la cual ayuda a la toma de decisiones, pero no decide

[1] Auditoría/http://www.monografias.com/trabajos32/auditoría.shtml[consulta 8 de mayo 2007]

por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoría informática.

Este cambio en el objetivo de la auditoría continuó desarrollándose, no sin oposición, hasta aproximadamente 1940. En este tiempo "Existía un cierto grado de acuerdo en que el auditor podía y debería no ocuparse primordialmente de la detección de fraude". El objetivo primordial de una auditoría independiente debe ser la revisión de la posición financiera y de los resultados de operación como se indica en los estados financieros de los clientes, de manera que pueda ofrecerse una opinión sobre la adecuación de estas presentaciones a las partes interesadas[2].

1.2. AUDITORÍA INFORMATICA.

1.2.1. Concepto.

Es el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas y de acuerdo a las normativas informáticas y generales en la organización”[3].

---

[2] Auditoría http://www.monografias.com/trabajos32/auditoría.shtml[consulta 8 de mayo 2007]

[3] Alvin A. Arens. Año 1985. Auditoría un enfoque Integral paginas 65-70

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones[3].

1.2.2. Objetivos.

Los objetivos de la auditoria informática son:

1.2.2.1. Seguridad de la información.

Seguridad de la información tiene tres líneas básicas en la auditoría del sistema de información:

a. Aspectos generales relativos a la seguridad.
b. Aspectos relativos a la confidencialidad y seguridad de la información.
c. Aspectos jurídicos y económicos relativos a la seguridad de la información.

1.2.2.2. Eficacia del sistema.

Eficacia del Sistema, esta vendrá determinada, básicamente, por la aportación a la empresa de una información válida, exacta, completa, actualizada y oportuna que ayude a la adopción de decisiones, y todo ello medido en términos de calidad, plazo y costo.

1.2.2.3. Rentabilidad del sistema.

La rentabilidad del sistema debe ser medida mediante el análisis de tres valores fundamentales: la evaluación de los costes actuales, la comparación de esos costes actuales con magnitudes representativas de la organización, y la comparación de los costes del sistema de información de la empresa con los de empresas similares, preferentemente del mismo sector de actividad.

1.2.2.4. Operatividad.

La operatividad es una función de mínimos consistente en que la organización y las maquinas funcionen[4].

[4] Auditoría de sistemas y desarrollo/http://www.monografias.com/trabajos40/auditoría-aplicacion[consulta 9 de mayo 2007]

1.2.3. Características.

La auditoría de informática puede dividirse en áreas de aplicación por lo que esta sirve para englobar las actividades que se han de auditar; pudiendo considerar que para que se realice en las diferentes áreas, se debe de observar la existencia de problemas, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas[5].

1.2.4. Importancia

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

---

[5] Auditoría de sistemas y desarrollo http://www.monografias.com/trabajos40/aplicación/auditoría[consulta 9 de mayo 2007]

1.2.5. Leyes y regulaciones aplicables.

1.2.5.1. Nivel internacional.

a) **COBIT (ISACA):**

Es la asociación líder en Auditoría de Sistemas, con 23,000 miembros en 100 países. ISACA propone la metodología COBIT ® (Control Objectives for Information and related Technology).
Es un documento realizado en el año de 1996 y revisado posteriormente, dirigido a auditores, administradores y usuarios de sistemas de información, que tiene como objetivos de control la efectividad y la eficiencia de las operaciones; confidencialidad e integridad de la información financiera y el cumplimiento de las leyes y regulaciones[6].
Por lo tanto, COBIT está diseñado para ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas[7]. En la actualidad se posee la versión 4.0 de COBIT[8]

b) **COSO:**

The Committee of Sponsoring Organizations of the Tread way Commission's Internal Control – Integrated Framework (COSO).

[6] Auditoría informática http://www.monografias.com/trabajos05/ aplicación/auditoría [consulta 15 de mayo 2007]

Publicado en 1992 hace recomendaciones a los contables de gestión de cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo de control la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones que explica en los componentes del ambiente de control, valoración de riesgos, actividades de control, información y comunicación y el monitoreo.

c) **NIA (IFAC):**

La Federación Internacional de Contables IFAC (http://www.ifac.org/) emitió las Normas internacionales de auditoría NIA.

IFAC muestra en las NIAs la auditoría en entornos informatizados y es una referencia a los controles para procesamiento electrónico de datos y la necesidad de estos cuando se esta en ambientes donde los instrumentos tradicionales del papel y demás pistas de auditoría no son visibles para los contables en el momento de realizar su trabajo.

d) **Normas generales para la auditoría de los sistemas de información (NASI)(ISACA).**

Emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información.

---

[7] http://www.monografias.com/trabajos40/ aplicación/auditoría[consulta 9 de mayo 2007]

La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditoría, requieren el desarrollo y la promulgación de Normas generales para la auditoría de los sistemas de información. La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. Las normas promulgadas por la Asociación de Auditoría y control de sistemas de información son aplicables al trabajo de auditoría realizado por miembros de la Asociación y por las personas que han recibido la designación de auditor certificado de sistemas de información[9].

1.2.5.2 Nivel Nacional.

a) **Ley de Propiedad Intelectual.**

Con fecha 14 de octubre de 1998, el Congreso de la Nación sancionó la ley que modifica y amplia la Ley de Propiedad Intelectual. La importancia de esta norma radica en que

---

[8] http://www.monografias.com/trabajos40/ aplicación/auditoría[consulta 9 de mayo 2007]

9 Auditoría informática http://www.monografias.com/trabajos05/ aplicación/auditoría [consulta 15 de mayo 2007]

incorpora a los programas de computación y a las compilaciones de datos dentro de las obras tuteladas por la Ley de Propiedad Intelectual, brindando protección a los derechos intelectuales de los creadores de software bajo el régimen del derecho de autor.

Esta ley, a la que se ha dado en llamar "Ley del Software", vino a llenar un importante vacío legislativo. Así, al incluir a los programas de computación dentro de los derechos de autor brinda protección desde la perspectiva civil, posibilitando al titular del derecho de propiedad intelectual accionar por daños y perjuicios contra aquel que utilice o reproduzca el programa sin su autorización y además, tipifica el delito de reproducción ilegal de programas de computación, al incluir la conducta dentro del tipo previsto por el art. 172 del Código Penal.

Tradicionalmente, no han existido mayores polémicas en lo que se refiere a la protección de los derechos intelectuales de los creadores de componentes del hardware y ello es debido a que las creaciones que se producen en tal terreno se encuentran comprendidas, por regla general, dentro de los llamados "inventos patentables". Por lo tanto, si el titular del derecho de propiedad intelectual cumple con los requisitos formales de patentamiento establecidos en la legislación, la protección se encontrará dada por las leyes de patentes[10].

[10] Propiedad Industrial.http://www.delitosinformaticos/auditoría shtml[consulta 23 mayo 2007]

1.2.6. Requerimientos del auditor informático.

El auditor de sistema tiene que cumplir con los siguientes requerimientos:

a) Entendimiento global e integral del negocio, de sus puntos claves, áreas críticas, entorno económico, social y político.
b) Entendimiento del efecto de los sistemas en la organización.
c) Entendimiento de los objetivos de la auditoría.
d) Conocimiento de los recursos de computación de la empresa.
e) Conocimiento de los proyectos de sistemas[11].

1.2.7. Clasificación de auditoría informática.[12]

1.2.7.1. Auditoría externa.

Aplicando el concepto general, se puede decir que la auditoría externa es el examen crítico, sistemático y detallado de un sistema de una unidad económica, realizado por un Contador Público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del

---

[11] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

[12] Auditoría.http://www.monografias.com/trabajos40/ aplicación/consulta 9 de mayo 2007]

mismo y formular sugerencias para su mejoramiento.

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

1.2.7.2. Auditoría interna

La auditoría interna es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la misma. La imparcialidad e independencia absolutas no son posibles en el caso del auditor interno, puesto que no puede divorciarse completamente de la influencia de la alta administración y aunque mantenga una actitud independiente como debe ser, esta puede ser cuestionada ante los ojos de los terceros.

1.2.8. Tipos de auditoría informática.[13]

TIPOS DE AUDITORÍA INFORMATICA

- Auditoría informática de producción o explotación
- Auditoría informática de desarrollo de proyectos
- Auditoría informática de sistemas
- Auditoría informática de comunicaciones y redes
- Auditoría de la seguridad informática
- Auditoría informática para aplicaciones en internet.
- Auditoría a los planes de desarrollo empresarial

1.2.8.1. Auditoría informática de producción o explotación[14]

En algunos casos también conocida como de explotación u operación, se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc.

---

[13] Auditoría http://www.monografias.com/trabajos32/auditoría.shtml[consulta 8 de mayo 2007]

[14] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

1.2.8.2. Auditoría informática de desarrollo de proyectos.

La función de desarrollo es una evolución del llamado análisis y programación de sistemas, y abarca muchas áreas, como lo son: prerrequisitos del usuario y del entorno, análisis funcional, diseño, análisis orgánico (reprogramación y programación), pruebas entrega a explotación o producción y alta para el proceso[15].

1.2.8.3 Auditoría informática de sistemas.

Se ocupa de analizar y revisar los controles y efectividad de la actividad que se conoce como técnicas de sistemas en todas sus facetas y se enfoca principalmente en el entorno general de sistemas, el cual incluye sistemas operativos, software básico, aplicaciones, administración de base de datos, etc.[16]

1.2.8.4 Auditoría informática de comunicaciones y redes.

Este tipo de revisión se enfoca en las redes, líneas, concentradores, multiplexores, etc. Así pues, la auditoría informática ha de analizar situaciones y hechos algunas veces alejados entre sí, y está condicionada a la participación de la empresa telefónica que presta el soporte. Para este tipo de

[15] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

[16] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

auditoría se requiere un equipo de especialistas y expertos en comunicaciones y redes[17].

1.2.8.5. Auditoría de la seguridad informática.

La auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, robos sabotajes, catástrofes naturales, etc.[18]

1.2.8.6. Auditoría informática para aplicaciones en internet.

En este tipo de revisiones, se enfoca principalmente en verificar los siguientes aspectos, los cuales no puede pasar por alto el auditor informático:

a) Evaluación de los riesgos de Internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
b) Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.

---

[17] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]
[18] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

c) Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers[19].

1.2.8.7. Auditoría a los planes de desarrollo empresarial.

La acción de planear las actividades permite al individuo fijarse metas, delinear los cursos de las acciones a seguir, establecer las reglas, fijarse objetivos a alcanzar, establecer las políticas que deban normar las operaciones y reglamentándolas en sistemas, métodos y procedimiento, que ayuden al logro de los objetivos[20].

1.2.9. Riesgos asociados al área de tecnología de información (Ti)[21]:

a) **Hardware.**

- Descuido o falta de protección: Condiciones inapropiadas, mal manejo, no observancia de las normas.
- Destrucción.

---

[19] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

[20] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

[21] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

b) **Software.**

- uso o acceso, copia, modificación, destrucción, hurto.
- errores u omisiones.

c) A**rchivos**

- Usos o acceso,
- copia, modificación, destrucción, hurto.

d) **Organización**

- Inadecuada: no funcional, sin división de funciones.
- Falta de seguridad,
- Falta de políticas y planes.

e) **Personal**

- Deshonesto, incompetente y descontento.

f) **Usuarios**

- Enmascaramiento, falta de autorización, falta de conocimiento de su función.

1.2.10. Otros riesgos asociados al sistema[22]

Los principales riesgos informáticos de los negocios son los siguientes:

[22] Auditoría de la Tecnología de Información http://www.monografias.com /A&C Consultaría y Auditoría Empresarial, Colombia[consulta 14 mayo 2007]

1.2.10.1. Riesgos de integridad

Abarca todos los riesgos asociados con la autorización, totalidad y exactitud de la entrada, procesamiento y reporte de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento del negocio y están presentes en múltiples lugares y múltiples momentos en todas partes de las aplicaciones; no obstante, estos riesgos se manifiestan en los siguientes componentes de un sistema:

a) **Interfaz del usuario:** Los riesgos en esta área generalmente se relacionan con la restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta su necesidades de trabajo y una razonable segregación de funciones. Otros riesgos en esta área se relacionan con controles que aseguren la validez y totalidad de la información introducida dentro de un sistema.

b) **Procesamiento:** Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles de detección (que son ex post) y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.

c) **Procesamiento de errores:** Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (excepción) sea capturado adecuadamente, corregido y reprocesados con exactitud completamente.

d) **Interfaz:** Los riesgos en esta área generalmente se relacionan con controles preventivos y de detección que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.

e) **Administrador de cambios:** Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuada de procesos de cambios organizacionales que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de procesos y la forma de comunicarlos e implementarlos.

f) **Información:** Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos. La integridad puede perderse por: errores de programación (buena información es procesada por programas mal construidos),

procesamiento de errores (transacciones incorrectamente procesadas) o administración y procesamiento de errores (administración pobre del mantenimiento de sistemas).

1.2.10.2. Riesgos de relación

Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (información y datos correctos de una persona/proceso/sistema en el tiempo preciso permiten tomar decisiones correctas.

1.2.10.3 Riesgos de acceso

Los riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: los de segregación inapropiada de trabajo, los asociados con la integridad de la información de sistemas de bases de datos y los asociados con la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

a) **Procesos de negocio:** Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.

b) **Aplicación:** La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.
c) **Administración de la información:** El mecanismo provee a los usuarios acceso a la información específica de entorno.
d) **Entorno de procesamiento:** Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.
e) **Redes:** En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.
f) **Nivel físico:** Protección física de dispositivos y un apropiado acceso a ellos.

1.2.10.4. Riesgos de utilidad

Los riesgos se enfocan en 3 diferentes niveles de riesgo:

a) Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
b) Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
c) Backups y planes de contingencia controlan desastres en el procesamiento de la información.

1.2.10.5. Riesgos de infraestructura

Estos riesgos se refieren a que en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente), pago de cuentas, etc.). Estos riesgos se consideran en el contexto de los siguientes procesos informáticos.

a) **Planeación organizacional:** Los procesos en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio. Además, verifica si existe una adecuada organización (gente, procesos), asegura que los esfuerzos de la tecnología informática sean exitosos.
b) **Definición de las aplicaciones:** Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio. Estos abarcan: la determinación de comprar una aplicación ya existente o desarrollar soluciones a la medida; también aseguran que cualquier cambio a las aplicaciones (compradas o desarrolladas) sigue un paso definido que confirma que los puntos críticos de proceso/control son consistentes (todos los

cambios son examinados por usuarios antes de la implementación).

c) **Administración de seguridad:** Los procesos en esta área aseguran que la organización esta adecuadamente orientada a establecer, mantener y monitorear un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización y a la reducción de fraudes a niveles aceptables.

d) **Operaciones de red y computacionales:** Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, además las responsabilidades de procesamiento de información son ejecutadas por personal operativo definido. También verificar que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.

e) **Administración de sistemas de bases de datos:** Los procesos en esta área están diseñados para asegurar que las bases de datos usados para soportar aplicaciones críticas y reportes tengan consistencia de definición, correspondan a los requerimientos y reduzcan el potencial de redundancia.

f) **Información/negocio:** Los procesos en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesiten.

1.2.10.6. Riesgos de seguridad general

Se pueden catalogar como aquellos a los que esta expuesto cualquier elemento de tecnología siendo los siguientes:

a) Riesgos de choque eléctrico: Niveles altos de voltaje.
b) Riesgos de incendio: Inflamabilidad de materiales.
c) Riesgos de niveles inadecuados de energía eléctrica.
d) Riesgos de radiaciones: Ondas de ruido, ultrasónicas y láser.
e) Riesgo mecánico: Inestabilidad de la piezas eléctricas.

1.3. AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS.

1.3.1. Concepto o definición

La auditoría informática en el desarrollo de proyectos es el conjunto de procedimientos y técnicas aplicadas en una evaluación, sistemática de las fases de análisis y programación de sistemas y de sus aplicaciones, con la finalidad optimizar recursos, lograr la satisfacción de los usuarios, comprobar la seguridad del sistema y garantizar que lo ejecutado por la maquina es lo previsto por el usuario.

1.3.2. Objetivos

1.3.2.1. Objetivo general.

a) Asegurarse de que el sistema marche conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.
b) Evaluar de forma integral el sistema que se encuentra en la fase de desarrollo.
c) Verificar si en los manuales se cumplen de los requerimientos y estos contribuirán a los diferentes usuarios del sistema.
d) Existir una planificación adecuada en la parte de entrenamiento y capacitación.
e) Facilitar el desarrollo de la prueba piloto y la implementación del sistema.

1.3.2.1. Objetivo específicos.

a) Identificar inexactitudes, ambigüedades y omisiones en las especificaciones(etapa de Análisis).
b) Descubrir errores, debilidades, omisiones antes de iniciar la codificación (Etapa de diseño).
c) Buscar la claridad, modularidad y verificar con base en las especificaciones. (Etapa de Programación).

d) Evaluar los controles de calidad en acceso, procesamiento y salida de información.
e) Verificar que se mantenga la integridad de los datos que el sistema almacena.
f) Evaluar los controles y niveles de seguridad establecidos para el acceso y uso de las aplicaciones informáticas.
g) Revisar los manuales considerando si cumplen con la ilustración adecuada para cada usuario.
h) Verificar si los manuales son de fácil comprensión para los usuarios finales.
i) Analizar si los manuales están completos y cumplen con los objetivos.
j) Verificar Metodología a seguir en la capacitación del personal.
k) Corroborar que se cumpla lo acordado en los contratos de capacitación.
l) Indagar sobre los materiales que se han proporcionado en la capacitación, si cumplen con los objetivos.
m) Verificar el proceso de inducción de los usuarios.

1.3.3. Finalidad

La finalidad de la auditoria informática en el desarrollo de proyectos es la optimización de los recursos tecnológicos, económicos, también lograr la satisfacción de los usuarios,

comprobar la seguridad del sistema y garantizar que el sistema ejecute cumple con los requisitos de los usuarios.

También la evaluación de la fase de desarrollo asegura que el sistema cumpla con las características siguientes:

i. Efectividad.
ii. Eficiencia.
iii. Integridad.
iv. Disponibilidad.
v. Cumplimiento.
vi. Confidencialidad.
vii. Confiabilidad.

1.3.4. Ventajas y desventajas.

1.3.4.1. Ventajas:

a) Se evalúa el desarrollo de las transacciones desde distintos puntos de vista, ya que la gestión obtendrá información oportuna y confiable para la toma de decisiones.
b) Clarifican los objetivos y facilitan el análisis estratégico.
c) Permite valorar si el sistema es comprensible para los usuarios y satisface sus necesidades.
d) Se puede identificar las fortalezas y debilidades en el proceso de desarrollo para corregirlas oportunamente.
e) Se verifica que el proceso de desarrollo se haga de forma coordinada y organizada.

f) Verificar si los costos y el tiempo invertido en del desarrollo de proyectos es el estipulado.
g) Verificar la seguridad lógica, física y la confidencialidad desde esta etapa.
h) Constata la coordinación y comunicación entre el personal involucrado en el proceso del ciclo de vida del desarrollo de sistemas
i) Confirma la existencia de documentación del sistema y que esta sea adecuada.

1.3.4.2. Desventajas:

a) La fase de Desarrollo de un sistema consume parte de recursos tecnificados, ya que existe poca aplicación o conocimiento del sistema.
b) El costo de adquisición y mantenimiento de una auditoría de sistemas es elevado.[23]

1.3.5. Etapas de la fase de desarrollo de sistema

El Desarrollar y probar programas, toma mucho tiempo. La instalación y la transferencia de datos también puede ser un proceso prolongado, dependiendo del tamaño de la institución.

[23] Capitulo 2 Conceptos básicos de Sistemas, año 2001 Paginas 54-58

Las etapas en esta fase no tienen que seguir una secuencia y cada una puede tomar bastante tiempo. Por lo tanto, donde sea posible, las etapas deberán coincidir para minimizar la duración total del proceso de desarrollo e implementación del sistema. El orden, el momento y la duración de las etapas deberán ser detallados en el plan del SIC establecido por el equipo del proyecto.

1.3.5.1. Etapa 1: Desarrollo del programa

La modificación de un programa existente o el desarrollo de uno personalizado requerirán de una fase de desarrollo del programa que puede tener una duración de una semana hasta un año. Es importante contar con un plan que detalle las etapas en el desarrollo del programa y que permita la retroalimentación temprana y frecuente por parte de los usuarios. A medida que se procede con el desarrollo y se aclaran algunos aspectos y limitaciones, los parámetros de diseño definidos en la fase 2 podrían tener que ser revisados.

1.3.5.2. Etapa 2: Instalación del equipo

La instalación del equipo de cómputo para un nuevo sistema puede consumir mucho tiempo y requiere de mucho planeamiento anticipado, particularmente en lo que se requiere a las decisiones de compra. Adicionalmente a la selección y

adquisición de las computadoras, impresoras, fuentes de poder, unidades de salvaguardia, cables y otros periféricos el plan deberá considerar lo siguiente:

a) La fuente de electricidad, incluyendo las conexiones a tierra.
b) Fuentes de poder de emergencia.
c) Las conexiones telefónicas.
d) La instalación de los cables para las redes.
e) Control de la temperatura, polvo y humedad.
f) La remodelación de las áreas de trabajo, especialmente los mostradores de atención al público.
g) Seguridad y acceso a los servidores y terminales.
h) Dispositivos de seguridad contra robos.
i) Extintores de incendios.

1.3.5.3. Etapa 3: Preparación y revisión de la documentación

A medida que se completa el diseño del sistema y se empieza con el desarrollo del mismo, puede procederse con la documentación del sistema. Una buena documentación puede ser invalorable para asegurar el uso adecuado del sistema, especialmente si se trata de instituciones grandes y descentralizadas o de instituciones que están pasando por un proceso de expansión. También puede ser útil para la capacitación del personal nuevo y para asistir al personal que enfrenta situaciones nuevas.

La documentación sobre políticas y procedimientos tendrá que ser revisada para que refleje los cambios introducidos por el nuevo sistema y por lo tanto tendrá que prepararse nueva documentación sobre el sistema.

1.3.5.4. Etapa 4: Configuración del sistema

Muchos programas instalados en más de una institución utilizan opciones de configuración para adaptar el sistema a las necesidades de la institución. Las opciones de configuración generalmente funcionan sobre la base de un menú y son accesibles por el usuario registrado al nivel de administrador de sistemas. Otras opciones de configuración menos comunes son activadas por códigos especiales ingresados al archivo de configuración por un técnico que está familiarizado con el programa.

La configuración consiste principalmente de los siguientes pasos:

a) Instalación de la estructura del plan de cuentas. Esta tarea crucial puede requerir la modificación del plan de cuentas de la institución para poder adaptarlo al programa.
b) Establecimiento de convenciones numéricas para las cuentas de clientes, de cobros y determinación de costos.

c) Establecimiento de relaciones o interfases entre los módulos relacionados — por ejemplo, para compartir y consolidar la información.

1.3.5.5. Etapa 5: Prueba

La siguiente etapa consiste en probar el sistema con los datos reales. Deberá ingresarse al sistema la información histórica de los meses pasados sobre unas 50 a 100 cuentas por cada tipo de producto.

Esta fase de prueba cumple dos propósitos. Primero, permite el desarrollo de una estrategia para la conversión de datos o para el ingreso de los datos iniciales para todas las cuentas activas Segundo, permite el estudio cuidadoso del comportamiento del sistema:

¿Se están calculando de manera adecuada los costos de servicios médicos, la facturación por la venta de servicios, las multas y la morosidad?

¿El sistema colapsa sin ninguna razón aparente?

¿Funciona de manera adecuada la red?

¿Permite el sistema corregir los datos ingresados erróneamente?

¿Se trata de un sistema de fácil utilización o presenta aspectos que necesitan ser resueltos con urgencia?

Deberán desarrollarse rutinas independientes de comprobación y auditoría para verificar que el sistema esté funcionando bien. Estas rutinas deberán detectar los campos que se encuentren vacíos de datos, los datos que se encuentren fuera de los rangos mínimos y máximos establecidos, la numeración secuencial, los números de cuentas o de clientes duplicados, los registros duplicados, los beneficiarios de empleados, particulares, fraudes por cotizantes (los registros de una tabla en una base de datos que no sean iguales a los registros de otras tablas), así como la veracidad del cálculo de depreciación, medicamentos. Muchos errores ocurren en las bases de datos como resultado de defectos en el programa, de la corrupción de la base de datos y por errores en el ingreso de los datos. Sin esta rutina de auditoría, los errores serán frecuentes, lo cual hará que disminuya la confianza que tiene el personal en el sistema.

1.3.5.6. Etapa 6: Transferencia de los datos

La transferencia de los datos es uno de los mayores imponderables en la instalación de un SIC. Requiere de decisiones cuidadosas y premeditadas, así como de la orientación, preferiblemente de un experto que conoce bien este campo.

Cuando se instala un programa comercial es mejor obtener consejo de un técnico familiarizado con el sistema. El riesgo puede ser enorme, una decisión errónea puede significar semanas de tiempo perdido porque los datos tendrán que ser ingresados nuevamente o meses de frustraciones porque los saldos y los cálculos no reflejan la realidad.

El primer problema es el de volumen. La introducción de nombres y de datos socioeconómicos de los clientes toma bastante tiempo. La información puede estar computarizada, pero generalmente se presentan incompatibilidades entre el SIC anterior y el nuevo en cuanto al tipo de información requerida o debido al formato donde la información será almacenada. Aunque es muy tentador transferir datos incompletos electrónicamente para luego ingresar manualmente los datos omitidos, este proceso puede requerir de un técnico especializado, lo cual puede resultar más costoso que simplemente asignar el ingreso manual de los datos a personal con un menor nivel de remuneración.

Los datos financieros pueden representar un problema aun mayor. Los datos en la mayor parte de las instituciones financieras están distorsionados, algunas veces seriamente. Por lo tanto, la instalación de un nuevo SIC se convierte en un ejercicio de auditoría exhaustivo — no necesariamente algo negativo, pero que incrementa sustancialmente el costo del SIC. Los saldos

iniciales en el mayor general deberán ser iguales a los saldos en los mayores auxiliares donde se detallan las cuentas de ahorros y préstamos. Los datos financieros deberán ser ingresados.

Es importante operar el nuevo sistema de manera procesado en grupos pequeños que incluyan menos de 50 cuentas. Los totales de los grupos deberán ser comparados manualmente con los expedientes y con los listados generados por computadora por el nuevo sistema.

Un tercer problema que viene a ser la fuente más importante de durante la transferencia de datos es la incompatibilidad en el tratamiento de los costos.

Es difícil predecir cuánto demorará o qué tan difícil será la transferencia de los datos, aun con una evaluación inicial cuidadosa. El ejemplo que se indica a continuación proporciona una idea general de lo que puede estar involucrado en este caso: La instalación de un SIC en una institución con 2 millones de cotizantes y con aproximadamente dos o tres beneficiarios cada uno requirió aproximadamente de 4 meses del personal para ingresar los datos.

Debido a que dos personas realizaron esta labor, el proceso tomó dieciséis semanas calendario de trabajo intensivo. También

requirió de la supervisión prácticamente a tiempo completo por parte de un técnico familiarizado con el programa.

1.3.5.7. Etapa 7: Capacitación

Un SIC con todas las aplicaciones posibles es un sistema complejo y su implementación requiere de grandes cambios en los procedimientos operativos de la institución. Por lo tanto, su instalación deberá estar complementada con un programa de capacitación intensivo para todo el personal. La capacitación por lo general toma de una a dos semanas, dependiendo de la complejidad del sistema y del número de personas que participarán.

Los usuarios deberán ser divididos en grupos, generalmente por departamentos. La capacitación de cada grupo deberá enfocarse en los aspectos de mayor importancia en sus respectivas áreas de operaciones, sin embargo, todos los participantes deberán recibir una visión panorámica sobre la operatividad de todo el sistema. La duración de la capacitación será variable, dependiendo nuevamente de la complejidad del sistema y de la experiencia que tenga el personal con sistemas similares. Es conveniente efectuar la capacitación diariamente en sesiones con una duración de una a dos horas.

El programa de capacitación deberá incluir los siguientes temas:

a) Organización del sistema, mantenimiento y procedimientos de salvaguardia.
b) Apertura y cierre de las cuentas de los clientes, determinación de costos así como la modificación y corrección de la información sobre los clientes y costos.
c) La responsabilidad de la empresa consultora o contratista de servicios informáticos no termina con la instalación del sistema para poder determinar los servicios.
d) Apertura de costos.
e) Recepción de pagos y depósitos por venta de servicios.
f) Corrección de las operaciones ingresadas erróneamente.
g) Transacciones registradas en las bases de datos.
h) Uso de módulos especializados (cuentas por cobrar, cuentas por pagar, inversiones, Recursos Humanos, Logística y Apoyo, Compras, Farmacia, Servicios básicos y Servicios de apoyo (incluye Alimentación y dietas, arsenal, lavandería, taller de impresiones y mantenimiento) Contabilidad y activos fijos).
i) Cierre diario, mensual y anual.
j) Preparación de estados financieros y reportes.
k) Uso de elaboradores de reportes.
l) Seguridad y procedimientos de control interno.

m) Procedimientos para arrancar nuevamente el sistema y para la recuperación de datos.[24]

1.3.6. Evaluación del control interno.

1.3.6.1. Estandarización de metodologías para el desarrollo de proyectos.

a) Asegurar que el beneficio de los sistemas sea el optimo
b) Elaborar estudios de factibilidad del sistema
c) Garantizar la eficiencia y eficacia en el análisis y diseño de sistemas.
d) Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema.
e) Optimizar el uso del sistema por medio de su documentación.

1.3.6.2. Comprensión de control interno.

Para comprender el control interno en esta fase es vital que presentemos los elementos siguientes:

a) Análisis del sistema actual
b) Diseño conceptual.

---

[24] Auditoría de un sistema informático, www.gestiopolis.com [consulta el 08 junio 2007]

c) Diseño detallado.

d) Programación.

e) Pruebas y correcciones.

f) Documentación del sistema.

g) Capacitación de usuarios.

h) Implementación del sistema.

i) Liberación del sistema.

j) Mantenimiento.

Para obtener una estandarización de metodologías en el desarrollo de un sistema es necesario; Verificar y estandarizar las actividades relacionadas al sistema. Para esto es necesario establecer que existen múltiples metodologías de aplicación general para el desarrollo de este, ya que garantiza la uniformidad en la aplicación de cualquier sistema y contribuya en gran medida a la eficiencia en el uso de los recursos informáticos del área de sistemas.

1.3.7. Riesgos y materialidad de auditoria.

Se puede definir los riesgos de auditoría como aquellos riesgos de que la información pueda tener errores materiales o que el auditor de sistemas no pueda detectar un error que ha ocurrido.

Cuando se efectúa una auditoría al sistema de información deben de tenerse en cuenta distintos riesgos y se pueden clasificar según se detallan:

a) *Riesgo inherente:* Cuando un error material no se puede evitar que suceda por que no existen controles compensatorios relacionados que se puedan establecer.
b) *Riesgo de control*: Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno.
c) *Riesgo de detección*: Es el riesgo de que el auditor realice pruebas exitosas a partir de un procedimiento inadecuado. El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad los hay. La palabra "material" utilizada con cada uno de estos componentes o riesgos, se refiere a un error que debe considerarse significativo cuando se lleva a cabo en una auditoría.

Es necesario además comprobar el riesgo de los objetivos de control no alcanzados. Una revisión detallada de las medidas de desempeño incluidas en el plan de calidad y asegurar si éstas:

a) Son alcanzables.
b) Satisfacen los requerimientos de la empresa y de los usuarios.

c) Son medibles, una revisión detallada de una muestra de proyectos :

   i. Se ha cumplido con la metodología del ciclo de vida del desarrollo de sistemas.

   ii. Toda adaptación/escalamiento de la metodología del ciclo de vida del desarrollo de sistemas es apropiada y ha sido aprobada.

   iii. Se han obtenido aprobaciones en todos los puntos de revisión y por parte de todo el personal clave de control (por ejemplo, oficial de seguridad de TI, personal de aseguramiento de la calidad, representantes de los usuarios, etc.)

   iv. Se han dado una coordinación y comunicación estrechas entre los usuarios de TI y los que implementan el sistemas (internos o terceras partes)[25]

   v. El desarrollo/las modificaciones fueron terminados satisfactoria y oportunamente

   vi. Se terminaron los reportes apropiados de aseguramiento de la calidad y se llevaron a cabo las acciones correctivas necesarias de manera oportuna.

---

[25] O´ Briend, James. *Bases de los Sistemas de Información. http://monografias.com* [consulta el 6 de junio 2007]

Una revisión detallada de la manera en la que las pruebas de programas, sistemas y la documentación son preparadas, aprobadas y mantenidas; verificación de post-implementación de aseguramiento de la calidad para asegurar que los reportes considera el cumplimiento de las provisiones del proceso del ciclo de vida del desarrollo de sistemas, así como los aspectos de efectividad y calidad de los sistemas nuevos/modificados. Identificando, planes de calidad que no se relacionen con los planes a corto y largo plazo.

CAPITULO II METODOLOGÍA Y DIAGNOSTICO DE LA INVESTIGACIÓN

DISEÑO METODOLOGICO

2.1. Tipo de Investigación

La investigación de un sistema informático integrado en el sector medico/hospitalario, fue investigado por medio del enfoque **hipotético deductivo**, analizando desde una perspectiva teórica-normativa las causas fundamentales de la problemática; con el propósito de descubrir elementos específicos, que permitan plantear una alternativa de solución o control de las deficiencias que podrían contener los requerimientos de la entidad al momento de ser implementados.

2.2. Tipo de Estudio

Por la naturaleza del problema identificado y los objetivos planteados, el proceso de investigación exigió la aplicación de los siguientes tipos de estudio: descriptivo, analítico y explicativo; a fin, de determinar si la integridad y oportunidad de la información dependen de la aplicación de la auditoria de sistemas.

2.3. Unidad de Análisis

La investigación fue realizada a instituciones médico/ hospitalarias privadas y autónomas descentralizadas del Gobierno Central, siendo la unidad de observación las jefaturas de informática que se encuentran en la fase de desarrollo del sistema, ya que ellos fueron nuestra fuente de información para realizar dicho estudio.

2.4. Universo

Debido a que la población objeto de estudio son 8 instituciones se investigará el 100% de los hospitales privados y las instituciones autónomas descentralizadas del gobierno central, entrevistando a los gerentes de las unidades de informática y personal involucrado con el área de sistemas de los hospitales.

2.5. Instrumentos y técnicas utilizados en la investigación

Para realizar el trabajo de investigación, se utilizarón las siguientes técnicas:

2.5.1. Investigación documental

En la investigación, se aplicó para la recolección de datos *la documentación bibliográfica*, la cual se basa en información ya procesada sustentada en libros, documentos y otros; para obtener aspectos teóricos y conceptuales y *la documentación hemerográfica.*

2.5.2. Investigación de campo

Para el desarrollo de la investigación de campo, se utilizó la técnica de la encuesta utilizando como instrumento el cuestionario, ya que este facilitará la obtención de la información necesaria para realizar la investigación.

Encuesta: Se elaboró un cuestionario de 30 preguntas dirigido al personal de las unidades de informática, usuarios, consultores, programadores afines; con el objetivo de conocer los problemas, deficiencias y desviaciones en el desarrollo del sistema integrado, para determinar un mejor curso de acción que ayude significativamente a su gestión financiera en un momento determinado.

2.6. Procesamiento de la información

El procesamiento de la información se efectuó por medio del programa utilitario Excel, mediante la elaboración de una tabla en la cual se detalla el dato absoluto obtenido en cada pregunta; además en base a este se elaboró su grafico respectivo. Posteriormente se procedió a ordenar, codificar y vaciar en una matriz la información obtenida.

2.7. Análisis e interpretación de Datos

Para el análisis e interpretación de la información obtenida a través del cuestionario, se elaboró; además, un cuadro comparativo entre las respuestas; para determinar la situación actual de los hospitales privados y de las instituciones autónomas y descentralizadas del gobierno central y en que forma influiría la aplicación de auditoría informática.

2.8. Diagnóstico de la investigación

Después del análisis de la información se hizo un diagnóstico a fin de concluir sobre la situación actual en las unidades de informática de los hospitales privados y las instituciones autónomas descentralizadas del Gobierno Central.

La auditoría de sistemas en desarrollo es importante; debido a que a través de ella se pueden detectar errores en la configuración y parametrización del sistema que se requiere implementar, ya que es fuente de información para diferentes áreas, en tal sentido el diagnóstico se segmentó en las siguientes áreas:

2.8.1 Conocimiento de auditoria de sistemas

Conocimiento de las jefaturas de unidades de informática sobre la aplicación de auditoría a un sistema integrado en desarrollo.

CUADRO No.1

No. PREG.	CRITERIOS	JEF. UNIDADES INFORMATICA	FRECUENCIA RELATIVA
1	Jefaturas de unidades de informática que cuentan con una estructura organizativa que define las áreas claves de autoridad y responsabilidad	8	8/8
2	Unidades de informática que tienen sistemas de información en su centro de atención	8	8/8
3	Fases que identifican las jefaturas que poseen sistemas de información: a) Desarrollo e implementación b) Ejecución c) Todas las Anteriores(mas las fases de factibilidad y prueba piloto)	 3 1 4	 3/8 1/8 4/8
4	Jefaturas que aplican auditoría de sistemas al SIC (Sistema de Información Computarizado)	6	6/8
5	Áreas en que es aplicada la auditoria de sistemas		

	a) Contabilidad b) Costos c) Todas las anteriores(mas otras áreas como tesorería, inversiones, compras, etc)	1 1 6	1/8 1/8 6/8
7	La utilización que las jefaturas dan a la información que le genera los SIC: a) Toma de decisiones b) Control de la información c) Todas las anteriores(mas la planificación de servicios futuros)	 2 1 5	 2/8 1/8 5/8
8	Unidades de informática en los cuales intervienen en el diseño de los sistemas los programadores, los analistas y los usuarios	8	8/8
28	Existencia de comunicación y coordinación entre usuarios y desarrolladores del sistema	8	8/8
30	Jefaturas de unidades de informática que consideran que seria un beneficio un trabajo de investigación que tratara sobre la aplicación de auditoría a un sistema en desarrollo, enfocado a los servicios médicos/hospitalarios	8	8/8

El cuadro número uno se refiere al conocimiento de las jefaturas de unidades de informática sobre la aplicación de auditoría a un sistema integrado en desarrollo, de acuerdo a la investigación realizada se puede concluir que los centros de atención poseen una estructura organizativa que les permite definir las áreas claves de autoridad y responsabilidad, además se concluyó que las jefaturas poseen identificadas las fases de los sistemas que poseen; sin embargo, no todas las jefaturas cuentan con una auditoría de sistemas que les permita identificar los riesgos a

los que están expuestos en el desarrollo de un sistema. De acuerdo a la ponderación de la frecuencia de 6/8 ejecuta auditoría a la diferentes fases del sistema en todas sus áreas; sin embargo, existen unidades que carecen de dicho servicio lo cual limita el objetivo para el que fue implementado el sistema; ya que manifiestan que la información que obtienen de los SIC es utilizada en 5/8 que representa a jefaturas encuestadas para realizar desde la planificación de servicios futuros, ejecución, control y toma de decisiones de la administración, tomando en cuenta que dichas jefaturas representan un porcentaje sumamente significativo en relación al universo que se ha considerado en la investigación, sería necesaria la aplicación de una auditoria a los sistemas en forma general.

El hecho de que 6/8 de los encuestados realiza auditoría a los sistemas de información, es un indicador de que las jefaturas tienen la disposición de implementarla en todas sus áreas con el interés de poder brindar cierta eficiencia y eficacia en el desarrollo de los sistemas que poseen los centros de atención.

Un punto muy importante son las personas que intervienen en el diseño de un sistema para que este funcione de acuerdo a sus requerimientos. Las jefaturas encuestadas coincidieron en que los sistemas son diseñados en su conjunto por las partes interesadas; es decir, los programadores, los analistas y los usuarios, estos últimos son los que al final ejecutarán los

sistemas; sin embargo, esto no es suficiente para garantizar el buen funcionamiento de un sistema, por ello el total de las jefaturas de las unidades de informática piensan que beneficiaria un trabajo de investigación que facilite la aplicación a un sistema en desarrollo y les permita evaluar así, con mayor eficacia y eficiencia todos aquellos procedimientos que se dan dentro de las rutinas del software que ejecuta o procesa la información con el fin de corregir la información que pueda ser confundida o se pueda perder por cualquier mal procedimiento del recurso humano que se ejecute.

En síntesis puede concluirse que el conocimiento que las jefaturas poseen acerca de los sistemas informáticos que administran no es suficiente para asegurar que el desarrollo del sistema será la herramienta idónea para la toma de decisiones; por lo tanto, una auditoria informática vendría a contrarrestar ciertos procedimientos, para evitar sesgos que podrían convertirse en un riesgo para la entidad.

2.8.2 Controles y Políticas

Los controles y políticas que aplican al sistema en desarrollo, incluyendo aspectos relativos a la evaluación de la fase.

CUADRO No.2

No. PREG.	CRITERIOS	JEF. UNIDADES INFORMATICA	FRECUENCIA RELATIVA
11	Posee políticas de control en la fase de desarrollo de sistemas		
	a) Seguridad en acceso	2	2/8
	b) Todas las Anteriores	6	6/8
12	Aplican controles en las interfases y parametrizaciones		
	a) Definiciones de Interfases	1	1/8
	b) Documentación de interfases	1	1/8
	c) Todas la Anteriores	6	6/8
18	¿Las políticas se encuentran actualizadas y son del conocimiento del personal?		
	SI	5	5/8
	NO	3	3/8
21	¿Los controles aplicados en el desarrollo del sistema permitieron que esta fase se realizara de forma eficiente y eficaz?		
	SI	8	8/8
23	¿Se controlan las entradas de información de documentos fuentes?		
	SI	7	7/8
	NO	1	1/8
25	¿Mantiene un registro de anomalías del procesamiento de la información?		
	SI	5	5/8
	NO	3	3/8
26	¿Existen control de fallas de exactitud?		
	SI	5	5/8
	NO	3	3/8

Al evaluar los controles y políticas que aplican al sistema en desarrollo, incluyendo aspectos relativos a la evaluación de la

fase; se denota de forma general que se le presta importancia a dicho tema en el área informática; considerando que la totalidad de la unidad de estudio considera que los controles aplicados en el desarrollo del sistema se realiza de forma eficiente y eficaz; aunque las respuestas siguientes indicaron lo contrario, por lo se puede observar que 6/8 de las entidades en sus fases de desarrollo posee políticas en: el diseño de la recopilación de datos fuentes, especificaciones del programa, definición y documentación de requerimientos y seguridad de accesos; además se observa que 2/8 de la unidad de estudio le presta importancia solo a la seguridad de acceso, no prestando intereses a los otros aspectos de control; esto es perjudicial para que la fase de desarrollo se realice de forma eficiente; sin olvidar que un 3/8 no mantiene actualizadas las políticas de control contribuyendo a la deficiencia en el desarrollo del sistema.

En el proceso de parametrización y en las interfases 2/8 tienen controles y políticas limitadas, por lo que se muestra que el interés al momento de ejercer controles se realiza en áreas especificas como por ejemplo en la entrada de documentos fuentes ya que un 7/8 posee controles; dando lugar en este caso a que uno de cada ocho tenga la posibilidad de poseer errores.

Es importante destacar que un 3/8 no mantiene un registro de anomalías del procesamiento de la información; y no posee

control de fallas de exactitud; limitando con esto la capacidad de mejoras de las aplicaciones.

2.8.3 Manuales y capacitación al personal

La importancia de manuales adecuados al sistema los cuales deben de mantenerse actualizados,considerando también la capacitación coordinada al personal involucrado.

CUADRO No.3

No. PREG.	CRITERIOS	JEF. UNIDADES INFORMATICA	FRECUENCIA RELATIVA
14	¿Qué tipo de manuales poseen?		
	a) Usuario	1	1/8
	b) Sistema	1	1/8
	c) Operación	1	1/8
	d) Todos Los anteriores	5	5/8
17	¿Con que frecuencia reciben capacitaciones los usuarios del sistema?		
	a) No reciben	1	1/8
	b) Cada vez que haya modificación al sistema	7	7/8

Un 3/8 no le da la importancia a los manuales del sistema en desarrollo; ya que, no posee los ejemplares necesarios para garantizar su buen funcionamiento y posterior implementación; además se le da mayor importancia a la capacitación de los

usuarios en caso de un cambio por lo que 7/8 de la unidad de estudio manifiesta que la capacitación al personal se da de forma frecuente; por tanto, se considera que para el buen desarrollo de un sistema integrado se necesita de los manuales de: *usuario, sistema y operación*; asegurando con esto el buen uso de las aplicaciones y que los usuarios tengan a su alcance: Resumen de los sistemas y del ambiente, explicación de todas la entradas, programas, salidas e integración de todos los sistemas con otros sistemas; explicación de todas las pantallas de entrada y despliegue de datos; explicación de todos los mensajes de error y la respuesta apropiada, procedimientos y/o recursos de superación de problemas, información necesaria para: Rediseño de los procesos del negocio, desarrollo oportuno, procedimientos y controles de usuarios y operacionales, materiales de entrenamiento y administración de cambios; para que el sistema supla las necesidades de información oportuna.

2.8.4 Limitantes para la implementación de auditoría

Las limitantes que las jefaturas de las unidades de informática tienen con relación a la implementación de auditoria a un sistema en desarrollo.

CUADRO No.4

No. PREG.	CRITERIOS	JEF. UNIDADES INFORMATICA	FRECUENCIA RELATIVA
6	Es importante que exista una planificación adecuada en la fase del desarrollo		
	SI	8	8/8
9	Ventajas al aplicar auditoría a un sistema en desarrollo.		
	a) Control de la información	1	1/8
	b) Validación de datos	1	1/8
	c) Información oportuna	1	1/8
	d) Todas las ventajas	5	5/8
10	Deficiencias en no aplicar auditoría a un sistema en desarrollo		
	a) Genera información incompleta	2	2/8
	b) Sesgos en los estados financieros	1	1/8
	c) Varias deficiencias	5	5/8
15	Al implementar auditoría a un sistema en desarrollo, se obtendría información confiable para la toma de decisiones	8	8/8
16	Efectos que dificultaría la decisión sobre la aplicación de auditoría a un sistema en desarrollo		
	a) Costos elevados	3	3/8
	b) Desconocimiento de aplicación	3	3/8
	c) Procesos complejos	1	1/8
	d) Todos los efectos	1	1/8

El cuadro número cuatro muestra los datos de las limitantes de las jefaturas de las unidades de informática en relación a la implementación de auditoria a un sistema en desarrollo.

Básicamente esta área es muy importante con respecto a la auditoría de sistemas ya que es donde debe de existir una planificación adecuada en la fase de desarrollo, para que este

pueda cumplir con las metas propuestas; esta verifica sobre la disponibilidad de los procesos que se cumplan según lo requerido este representa el total, lo cual es muy importante debido a que todos los encuestados están de acuerdo en planificar sus actividades relacionadas a los sistemas en desarrollo.

También es necesario mencionar las ventajas que se obtienen al aplicar auditoría al sistema en desarrollo, entre las que podemos mencionar validación de datos, control de la información entre otras representan un 5/8 que incluye jefes de la unidad de informática; muy significativo ya que entre los encuestados certifican que es muy importante la aplicación de auditoria a un sistema en desarrollo; a futuro evitara problemas de configuraciones, parametrizaciones en el sistema y sobre todo les ahorrara tiempo y dinero.

Los encuestados opinaron sobre la incidencia en la no aplicación de auditoría a un sistema en desarrollo, 2/8 mencionan que la información que este genere será incompleta, porque siempre existen contingencias en la implementación del sistema.

Entre las propuestas de las incidencias que se plantearon 5/8 de los encuestados mencionan como la información incompleta, ocasionara sesgos en los estados financieros al emitir reportes al implementarse el sistema.

Al aplicar auditoría a un sistema en desarrollo, se obtendría información confiable para la toma de decisiones; al consultarle a los encuestados, todos certifican que sí es factible obtener información confiable, ya que al implementar el sistema los errores serían mínimos o nulos, puesto que la auditoría detectaría y corregiría antes de implementarlo.

Para finalizar el cuadro de las variables integradas tenemos los efectos que dificultarían la decisión sobre la aplicación de auditoría a un sistema en desarrollo, entre ellos podemos mencionar y quizás el mas importante son los costos elevados al aplicar auditoría de sistemas representa 3/8 de los encuestados, ya que hoy en día las instituciones no cuentan con un presupuesto asignado para este servicio. Aunque después de implementar el sistema tengan que pagar adicional por las eventualidades que surjan.

Como segundo rubro de gran impacto es el desconocimiento de aplicación de auditoría a un sistema en desarrollo, representa 3/8 muy significativo, esto se debe a que la mayoría de entidades desconocen la aplicación de auditoría, que es vital para un sistema informático.

Otro efecto que dificulta la aplicación de auditoria es que es un proceso complejo y representa 1/8 de las encuestas realizadas, hoy en día mencionan que los despachos casi no

ofertan este tipo de auditoría por no tener el personal idóneo y por los elevados costos económicos.

En función de lo antes expuesto en el diagnostico de la investigación se puede concluir que las jefaturas de las unidades de informática necesitan de la aplicación de auditoría de sistemas como una herramienta que le permita conocer los lineamientos básicos tanto a nivel teórico como a nivel practico, para efectos de poder tomar decisiones acertadas en las áreas involucradas. En tal sentido en el capitulo III de este trabajo se proporcionarán los lineamientos para poder evaluar y aplicar una auditoria a un sistema en desarrollo con cada una de las fases de la auditoría lo cual permitirá conocer diferentes procedimientos, técnicas y métodos que tanto las normas de auditoría de sistemas como las NIA´S establecen para planear, ejecutar, y emitir una opinión sobre la situación de los sistemas informáticos en desarrollo.

2.8.5 Control interno en un sistema en desarrollo

Los procedimientos y normas de control interno establecidos en el desarrollo del sistema que influyen en la administración de los riesgos.

CUADRO No.5

No. PREG.	CRITERIOS	JEF. UNIDADES INFORMATICA	FRECUENCIA RELATIVA
13	Procedimientos de evaluación que posee en la fase de entrada de datos		
	a) Validación de la información	2	2/8
	b) El usuario no puede manipular información	1	1/8
	c) Formatos prediseñados	2	2/8
	d) Todos los procesos de evaluación	3	3/8
19	Importancia de tener una buena administración de riesgo en el área del sistema	8	8/8
20	Existencia de normas que definen el contenido de los instructivos de captación de datos	8	8/8
22	Favorecería un plan sobre procedimientos y técnicas de evaluación del sistema integrado a los usuarios	8	8/8
24	Utilización de manual de control interno de las bases de datos.		
	a) Utiliza manual de control interno	6	6/8
	b) No utiliza manual de control interno	2	2/8
27	Los reportes de los requerimientos han sido preparados adecuadamente y en forma oportuna según lo esperado	8	8/8
29	Se ha considerado el rediseño del sistema		
	a) Se ha considerado el rediseño	3	3/8
	b) No se considero el rediseño del sistema	5	5/8

En la quinta parte del diagnóstico se aborda la importancia de los procedimientos y normas de control interno establecidos en el desarrollo del sistema que influyen en la administración de los riesgos.

Como primer punto tenemos la evaluación de los procesos en la fase de entradas que se clasificó en tres apartados siendo una

de ellas la validación de información con 2/8 significativo ya que en la aplicación de procesos es muy importante, la segunda con 1/8 se refiere a que el usuario no pueda manipular la información, esto lo podría efectuar si tiene acceso a archivos fuentes, es por ello que debe normarse según los perfiles del usuario para que pueda acceder a la información requerida.

Como tercer procedimiento de evaluación en la fase de entrada de datos tenemos los formatos prediseñados, estos son de gran importancia para el área de informática, ya que a través de ellos se verificará que el que diseño del sistema debe apegarse al requerimiento y cumplirlo a cabalidad según las especificaciones técnicas y funcionales establecidas por los usuario funcionales y al agrupar las evaluaciones entre los encuestados lanzó significativamente 3/8 lo que significa que esta fase en la auditoria a un sistema en desarrollo es una herramienta útil para la toma de decisiones.

Al establecer si existe una buena administración de riesgo en el área del sistemas el 100% de los encuestados manifestaron que es primordial que se establezca una buena administración de riesgos en el sistema, esto con el objetivo de prevenir, detectar y corregir a tiempo las contingencias que puedan ocurrir y tener planificadas las actividades para contrarrestar este tipo de eventualidades cuando se implemente el sistema.

Cabe mencionar que las áreas de riesgo son todas aquellas que se pueden prevenir y aquellas como desastres naturales donde el sistema tendrá que generar archivos automáticos de salvaguarda o el encargado del sistema realizar backup según la normativa establecida por la unidad de informática.

En este rubro todos de los encuestados manifestaron que es importante tomar en cuenta la existencia de normas que definan el contenido de los instructivos de captación de datos, ya que estos serán la guía técnica para las creaciones de bases de datos y captación; por lo tanto, debe estar normado y uniforme por ejemplo un formato deberá llevar identificado la institución, logo, dirección, los rangos de los caracteres al momento de ingresar una transacción.

De los encuestados la totalidad manifiesta que les favorecería un plan sobre procedimientos y técnicas de evaluación del sistema integrado a los usuarios, ya que por medio de ello podrían evaluar los perfiles y la idoneidad a cada usuario y asignarle por este medio los accesos según las autorizaciones que decida la unidad de informática.

Este procedimiento quizás sea el más importante ya que de los encuestados un 6/8 piensan que la importancia de poseer un manual de control interno para las bases de datos serviría a las jefaturas, para medir, controlar la información y además es la

técnica que se implementaría para los usuarios de informática sobre el uso adecuado de los manuales de control interno de las bases de datos en la red. Mientras que 2/8 manifiesta que actualmente no poseen un manual de control interno para evaluar dichas bases de datos, esto a nivel de informática es grave ya que si ocurriera algún plan que no lo tiene planificado no tendría un soporte de cómo evaluar las bases de datos, y es delicado ya que indica que no existe una guía de cómo manejar las bases de datos si no hubiere alguien que conozca el sistema.

Otro rubro muy importante son los reportes de los requerimientos de que si han sido preparados adecuadamente y en forma oportuna según lo esperado, todos de los encuestados manifestaron que los reportes fueron preparados adecuadamente según lo solicitado y a la necesidad de la institución.

Como ultimo punto tratamos sobre si la institución ha considerado el rediseño del sistema, 3/8 de los encuestados manifestó que sí lo han considerado, esto se debe a que existe información que no se tomo al inicio y hoy que han visualizado el sistema y las aplicaciones que tiene creen que es necesario ampliarlo para que cuando se implemente el usuario final tenga mayores oportunidades de aprender y de simplificar el trabajo. No obstante 5/8 manifestó que no han considerando el rediseño, ya que los requerimientos cumplen con las expectativas de la institución y de los usuarios funcionales y técnicos.

CAPITULO III: PROPUESTA PLANEACION DE AUDITORÍA DE SISTEMAS

3.1 ANTECEDENTES DE LA INSTITUCIÓN

3.1.1. Datos generales de la entidad

Nombre completo de la entidad	:	Instituto Salvadoreño del Seguro Social
NIT	:	0614-251045-002-0
Dirección	:	Alameda Juan Pablo II y 39 Avenida norte, torre admón.
Teléfono	:	2268-3000

3.1.2. Giro de la institución

Servicios de atención médica hospitalaria

3.1.3. Visión

Institución participativa, con organización funcional y liderazgo en la atención integral de salud que garantiza servicios de calidad, con personal comprometido con la misión institucional.

3.1.4. Misión

Brindar provisión de servicios integrales de salud y prestaciones económicas en forma oportuna, eficiente y excelente

trato humano, generado por una cultura institucional de servicio, que supere las expectativas del derechohabiente.

3.1.5. Valores

a) Universalidad
b) Equidad
c) Calidad
d) Solidaridad
e) Eficiencia
f) Calidez
g) Identidad

3.2. OBJETIVOS DE LA AUDITORÍA AL SISTEMA EN DESARROLLO.

3.2.1. Objetivo general.

Evaluar el sistema informático integrado SAP, a efecto que cumpla con los requerimientos solicitados en la fase de análisis y diseño, a través de la aplicación de auditoría en el desarrollo del mismo.

3.2.2. Objetivos específicos.

a) Realizar una revisión con el gerente de informática, jefe de mantenimiento de sistemas, jefe operativo de sistemas (analistas y programadores), técnicos y personal de digitación del departamento de informática, a fin de

evaluar las operaciones que se desarrollan en el sistema y la gestión administrativa del área de informática.

b) Verificar que las aplicaciones cumplan con las normativas y requisitos legales establecidos para la actividad que se controlan en las mismas; así como el cumplimiento de políticas y procedimientos que se llevan a cabo en las acciones del área y de los sistemas de procesamiento de información, de su personal y usuarios.

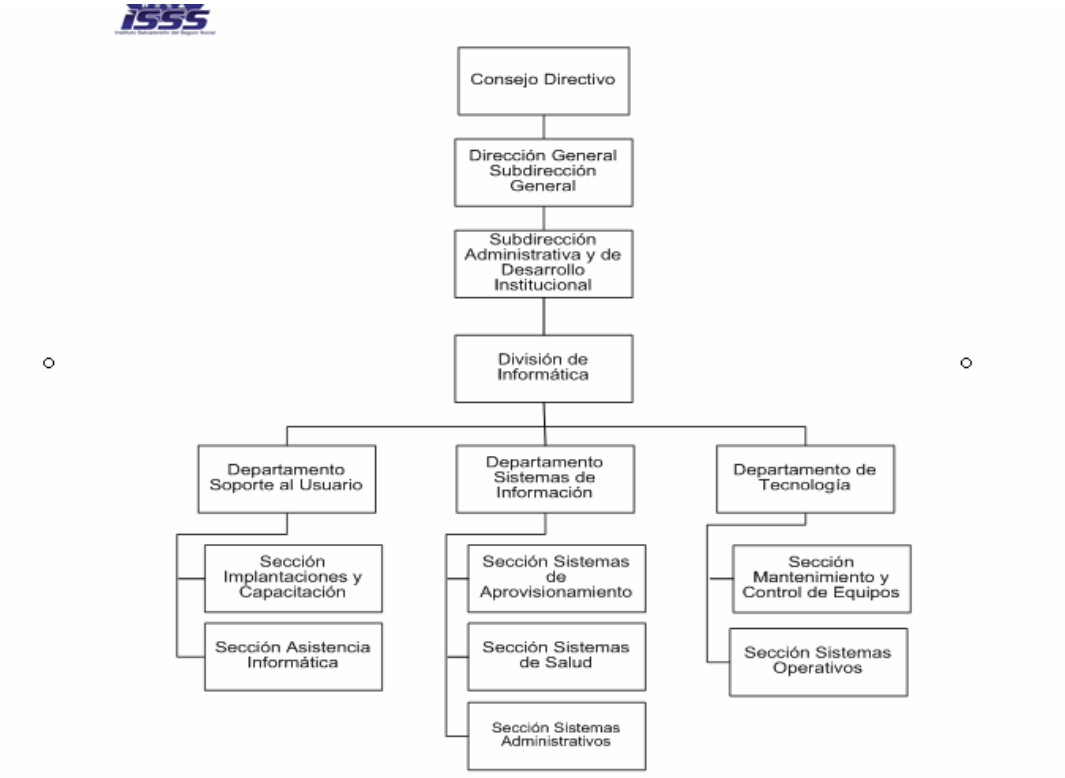
c) Evaluar los controles de acceso, procesamiento y salida de la información, orientado a mantener la integridad de los datos que deben almacenarse.

d) Evaluar los controles y niveles de seguridad establecido para el acceso y el uso de las aplicaciones informáticas que obtendrán los usuarios finales.

e) Examinar la información, documentación, registros de los sistemas y sus respectivas bases de datos.

3.3. INFORMACION DEL ÁREA DE SISTEMAS (CENTRO DE CÓMPUTO).

3.3.1. Estructura organizativa.



Fuente: estructura organizativa ISSS

La dependencia jerárquica de la división de informática cuenta con los siguientes departamentos ó áreas:

a) Soporte técnico

b) Sistemas de información

c) Tecnología

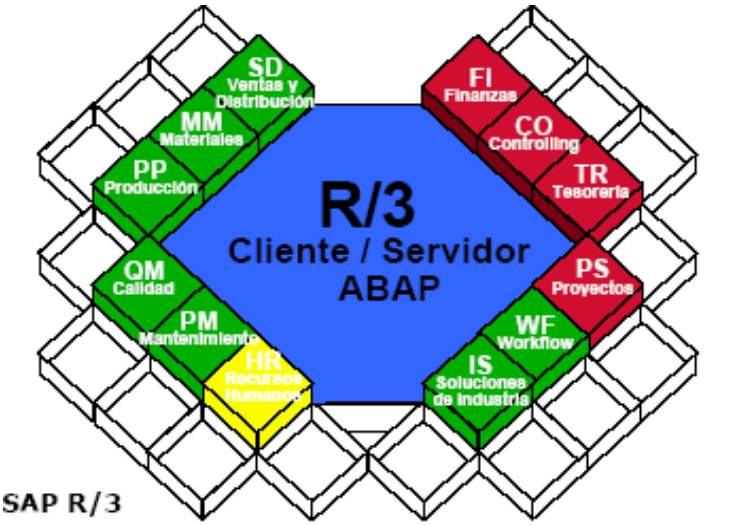
Tabla No 1: Cuadro resumen de la estructura organizativa de la división de informática

NOMBRE DE LA UNIDAD	DESCRIPCIÓN DE ACTIVIDADES	FINALIDAD	FUNCIONES PRINCIPALES	RESPONSABLES
a) **Soporte técnico al usuario:** el cual esta dividido en implantación y capacitación y asistencia informática.	1) Mantener y administrar las redes, sistemas y equipos informáticos 2) Capacitación y brindar asistencia personalizada al personal en tecnología que adquiera la institución	Diseñar y consolidar los criterios y esfuerzos destinados a los sistemas de información automatizada.	1) Monitorear el sistema a nivel institucional. 2) Apoyar computacionalmente las actividades de todas las direcciones, departamentos y otras unidades de la institución, preocupándose del desarrollo de programas como de la actualización de todo su equipo.	1) Jefatura del departamento de soporte al usuario. 2) Sección de Implantación y capacitaciones 3) Sección de asistencia informática. 4) Usuarios del sistema.

NOMBRE DE LA UNIDAD	DESCRIPCIÓN DE ACTIVIDADES	FINALIDAD	FUNCIONES PRINCIPALES	RESPONSABLES
b) **Sistemas de información**	Instalación y configuración de Hardware y Software en los distintos departamentos de la institución.	Supervisar todo proyecto informático que fuere contratado a terceros y ser la contraparte técnica de los sistemas computacionales arrendados.	1) Mantener los sistemas informáticos de la entidad y de los equipos computacionales. 2) Colaborar a la optimización de recursos y procedimientos administrativos, con el apoyo del hardware y/o software que sea necesario para poder acceder a la integración de diversidad de módulos. 3) Velar por la información registrada de los módulos de Contabilidad, Cuentas por cobrar, Cuentas por Pagar, Materiales, Tesorería, Compras, Contratos, Costos, Ventas, Recursos Humanos, Presupuestos, Planeamiento, etc. 4) Velar por la integridad de la información almacenada en equipos computacionales de su propiedad, además de elaborar y ejecutar los planes de contingencia necesarios en caso de pérdida de información. 5) Preparar y entregar la información estadística a las unidades que lo requieran.	1) Jefatura de Sistemas de información. 2) Sección de aprovisionamiento. 3) Sección de sistemas de salud. 4) Sección sistemas administrativos. 5) Usuarios del sistema.

NOMBRE DE LA UNIDAD	DESCRIPCIÓN DE ACTIVIDADES	FINALIDAD	FUNCIONES PRINCIPALES	RESPONSABLES
c) Tecnología	Mantenimiento y reparación de equipos, estructura física, lógica de las instalaciones.	Monitorear que los equipos funciones adecuadamente según las necesidades del usuario y la información que almacenara.	1) Controlar las concesiones que le corresponda n de acuerdo a su participación en la elaboración de las especificaciones técnicas y que sean necesarias a la naturaleza de sus funciones. 2) Crear y administrar las bases de datos que sean relevantes para la toma de decisión y para el conocimiento de la información. 3) Coordinar el accionar de las distintas dependencias a manera de ir integrando y correlacionando información y bases de datos. 4) Cumplir otras tareas que el Administrador le encomiende, de acuerdo a la naturaleza de sus funciones y Marco Legal.	1) Departamento de tecnología 2) Sección mantenimiento y control de equipos. 3) Sección sistemas operativo. 4) Usuarios del sistema.

Figura No 1: Descripción grafica del sistema SAP R/3



Fuente: División de informática

3.3.2. Ubicación geográfica.

Las instalaciones de la entidad se encuentran sobre alameda Juan Pablo II y 39 avenida norte, torre administrativa.

Las instalaciones poseen una infraestructura de doce niveles construidos en sistema mixto, el inmueble fue construido en 1981 resistiendo a la fecha a las adversidades ambientales a que se expone el país.

La institución cuenta con una unidad de informática ubicada en el primer nivel, sótano, con una ruta de acceso limitada, ya que es de suma importancia para la administración ya que el personal que ingresa al área es únicamente el que labora en ella.

3.3.3. Cantidad de empleados.

La división de informática cuenta con 68 empleados cada uno depende de distintas secciones, como se describen anteriormente en la estructura organizativa, en las que realizan diversidades de funciones de acuerdo a la experiencia que posee cada uno y de acuerdo al perfil por el cual fue contratado.

3.3.4. Personal que ocupara el sistema SAP

El personal que realizara transacciones en la entidad son todos aquellos usuarios finales capacitados y autorizados por las jefaturas correspondientes en donde se implemente el sistema en desarrollo.

3.3.5. Dependencias relacionadas.

La institución posee dependencia en cuanto a la información que se procesa en los diferentes departamentos de la siguiente manera:

a) ***Dependencias internas.***

El departamento de *recursos humanos* a través del modulo de nominas proporciona al departamento de Contabilidad toda la información relacionada a los pagos de planillas de los

empleados que prestan servicios en la institución, así como las diferentes prestaciones que se brindan a dichos empleados.

Tesorería proporciona información al departamento de Contabilidad sobre los egresos e ingresos de efectivo a la institución en forma diaria mediante el modulo de Tesorería.

Cuentas por cobrar brinda información de los saldos pendientes de cobro a los responsables para la adecuada toma de decisiones y compras contratos brinda información sobre los resultados de licitaciones que son aprobadas y hace proyecciones de las gestiones que se realizaran en un periodo determinado, para que el departamento de Contabilidad pueda tener una vista panorámica sobre el rendimiento actual de la institución.

Y en fin el departamento de *contabilidad* relaciona toda la información para distribuirla en los diferentes informes que proporcionara a los usuarios internos y externos, para la toma de decisiones, tomando en cuenta la importancia significativa que se tiene para el logro de los objetivos.

El proceso de información será muy factible ya que el sistema es muy amigable, en la pantalla le menciona las opciones y con solo

darle opción asignada el mismo sistema lo guía a elaborar lo que el usuario quiere.

El proceso para registrar un pedido, factura un costo es sencillo, ya que se ingresara la información requerida por los usuarios funcionales y al emitir los reportes se tendrán los que realmente son necesarios.

La salida de información es muy accesible ya que el sistema le da opciones donde solo al asignarle el numero que el usuario le asigne, así le reportara la información requerida.

b) ***Dependencias externas***

Las operaciones que se realizan dentro de la institución están basadas en la tecnología de punta, ya que cuenta con el servicio de redes bancarias para realizar transacciones de abonos en cuenta ajenas (proveedores, clientes) y se gestionan los diferentes pagos de planillas.

Esto conlleva a poder tener en el momento oportuno un estado de cuenta actualizado el cual sirve para tomar decisiones financieras adecuadas.

3.3.6. Datos estadísticos.

El sistema se ha proyectado emitir reportes e informes de una manera periódica, para las diferentes necesidades que se presentan en la institución, para la toma adecuada de decisiones y logro de objetivos planteados, según se muestra a continuación:

Tabla No 2: Datos estadísticos de emisión de reportes del Instituto Salvadoreño del Seguro Social

NOMBRE	FRECUENCIA				
	DIARIA	SEMANAL	QUINCENAL	MENSUAL	ANUAL
Reporte de disponibilidades.		X			
Reporte de cuentas por pagar.			X		
Reportes de cuentas por cobrar.		X			
Conciliaciones bancarias.				X	
Libro diario.				X	
Reporte de ventas.	X				
Reporte de compras.		X			
Balance general.					X
Estado de flujo de efectivo.					X
Estado de resultado.				X	
Estado de cambios en el patrimonio.					X
Reporte de inventario.		X			
Reporte de costo de venta de servicios médicos.				X	
Planillas de empleados.			X		

Reporte de retenciones.				X	
Listado de convenios firmados.					
Reporte de pacientes atendidos en entidades privadas.					
Reintegro de servicios médicos.					
Control de pacientes por mezclas parentérales.					

3.4. EVALUACION DE RIESGOS.

El sistema SAP tendrá la facilidad de utilizarlo, debido a que permite mediante el ingreso a distinto menús.

El sistema posee infinidad de opciones para poder retroalimentarlo y obtener a través de ello ilimitadas ventajas para el usuario en el sentido de que posee muchas herramientas que pueden utilizarse mal por algunos usuarios que no conozcan el sistema a implantar es por ello que se están tomando las medidas provisorias para asignarles a cada usuario final el acceso según el perfil autorizado por la jefatura.

El sistema de información posee riesgos asociados entre los que podemos mencionar.

3.4.1. Riesgos asociados.

Los riesgos asociados el sistema se pueden clasificar como riesgos relaciones con:

3.4.1.1. Los procedimientos y marco legal.

Los riesgos relacionados con los procedimientos y marco legal son:

a) Carencia de controles administrativos.

b) Planeación organizacional

c) Riesgos relacionados con la percepción de usuarios

d) Interfaz de usuario

e) Administración de cambios

f) Falta de conocimiento del usuario.

g) Personal capacitado.

h) Información suficiente apropiada.

i) Mal uso del sistema.

j) Personal contratado.

3.4.1.2. Los niveles de seguridad.

Riesgos relacionados con los niveles de seguridad del sistema:

a) ***Panorama físico:***

i. Cuidado del equipo.
ii. Resguardo físico del equipo, backup.
iii. Acceso al centro de cómputo.
iv. Tecnología.
v. Mantenimiento.
vi. Desastres naturales.

vii. Fraude.

viii. Hurto.

ix. Inflamabilidad de materiales.

x. Niveles de alto voltaje.

b) ***Panorama técnico:***

i. Lenguaje de programación incompatible con el sistema operativo.

ii. Falta de fuentes o ejecutables de la instalación.

iii. Falta de personal capacitado para la operatividad del sistema.

c) ***Panorama lógico:***

i. Acceso no autorizado a bases de datos.

ii. Pertinencia adecuada.

iii. Programación de actualización constante.

iv. Eficiencia (Alcance del Software).

v. Virus informáticos.

vi. Errores en el procesamiento de datos.

vii. Existencia de controles de acceso automatizados

d) ***Valores parametrizables del sistema:***

i. Falta de autorización de personal a parametrizar el sistema

ii. Continúa modificación de los parámetros del sistema.

iii. Falta de restricciones al acceso de parametrización.

e) ***Pistas de auditoría:***

i. Inexistencia de políticas relativa al vaciado frecuente de la información

ii. Falta de políticas para el proceso de adición, modificación y eliminación de registros.

3.4.1.3. El funcionamiento del sistema.

Los riesgos relacionados con el funcionamiento del sistema son:

a) **Origen de datos:**

i. Inadecuado procesamiento uniforme de las transacciones.

ii. Falta de secuencia seguida para el ingreso de datos al sistema

iii. Falta de encabezados descriptivos en la información.

iv. Inexistencia de espacios suficientes para correcciones y firmas responsables.

b) **Entrada de datos:**

i. Actualización o desfase en el ingreso de los datos.

ii. Realización de cálculos manuales previamente a ser ingresados al sistema.

iii. Formatos no predefinidos.

c) **Procesamiento de datos:**

i. Autorización al acceso de personal al código fuente.

ii. Utilización de la versión correcta del programa

iii. Caídas del sistema

d) **Salida de la información:**

i. Inexactitud e integridad en la información definida en los reportes.

ii. Falta de listados de fechas en que se generan los reportes.

iii. Inexistencia de procedimientos de destrucción o almacenamiento adecuado de los reportes con información restrictiva o confidencial.

3.4.1.4. Los planes de contingencia.

Los riesgos relacionados con los planes contingentes se puede observar en:

a) **Back up:**

i. Inexistencia de técnicas de recuperación, restauración usada para minimizar la ruptura de los sistemas.

ii. Inadecuados procedimientos de resguardo de la información.

iii. Inexistencia de periodos de respaldo y retención de la información.

b) **Lugares de resguardo:**

i. Falta de lugares apropiados para el resguardo de la información.

ii. Falta de políticas para la seguridad de la información.

Estos riesgos asociados al sistema en desarrollo solo se podrán evitar mediante una planificación adecuada del manejo del sistema pues mediante el esfuerzo, tiempo, recursos disponibles se podrá atacar los problemas.

También se puede manejar mediante un minucioso análisis de los riesgos y debilidades (FODA), esto nos permitirá identificar, definir y revisar los controles de seguridad.

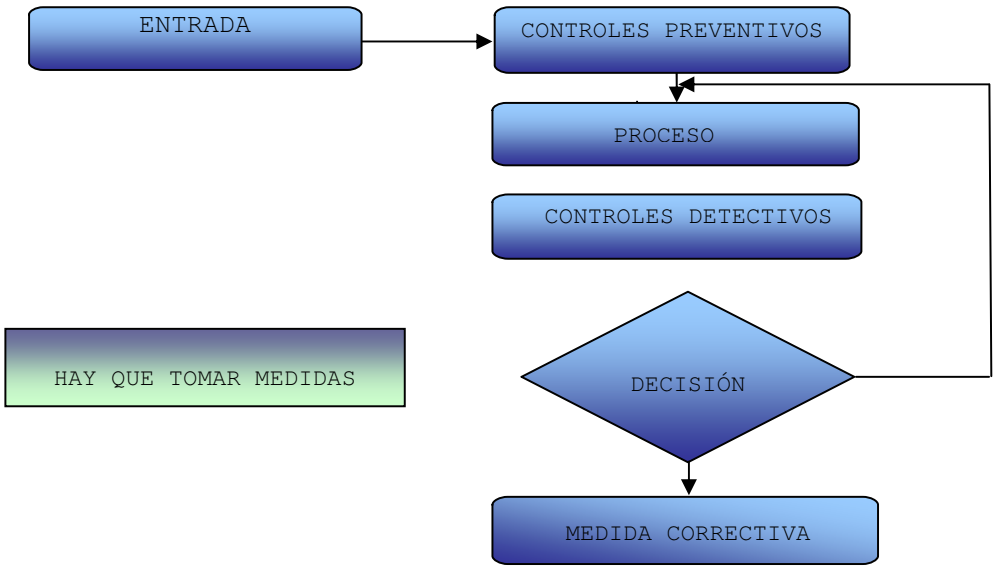
Es importante determinar mediante la planificación las debilidades que el sistema pueda tener con relación a la seguridad física, lógica, los parámetros de seguridad y los sitios de mayor peligro, se pueden hacer el mantenimiento más fácilmente.

Hoy en día con la tecnología de punta existente en el país el uso de la red por medio de internet se vuelve insegura ya que se

intercambia información muy importante y privada para la institución y se expone a la Web, por medio de ella puede interceptar datos de los que se están transfiriendo y los pueden observar, copiar, modificar la información confidencial de la institución.

3.4.2. Medidas de control en un sistema en desarrollo.

Figura No 2: organigrama de cómo se pueden llevar medidas de control en un sistema en desarrollo



3.4.3. Matriz de riesgos.

Es una herramienta fundamental para prevenir, detectar y corregir errores o sesgos que tenga el sistema tanto en las aplicaciones como en su entorno, esta nos permite obtener

señales, advertencias sobre los controles existentes y sobre todo la efectividad esperada según la planificación.

3.4.3.1 Riesgos de auditoría.

Se puede definir los riesgos de auditoría como aquellos en los cuales la información pueda tener errores materiales o que el auditor de sistemas no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera:

a) **Riesgo inherente:** Cuando un error material no se puede evitar que suceda por que no existen controles compensatorios relacionados que se puedan establecer.
b) **Riesgo de control:** Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno.
c) **Riesgo de detección:** Es el riesgo de que el auditor realice pruebas exitosas a partir de un procedimiento inadecuado.

Tabla No 3: Matriz de riesgo del sistema en su entorno interno

Causas de riesgos				
Controles	**Causa 1**	**Causa 2**	**Resultado causa**	**Clave de efectividad**
Supervisión de seguridad	Cuentas de usuarios triviales	Recursos compartidos	Causa 1	confiable

Software de antivirus	No clasificaron datos	No utilización de antivirus	Causa 2	Poco efectivo

Causas de riesgos	Infección en las carpetas	Acceso a información confidencial	Modificación de información
Recursos compartidos	SI	NO	SI
No utilización de antivirus	SI	NO	SI
No clasificación de datos	SI	SI	SI

3.4.4. La significatividad del componente (materialidad):

El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad los hay. La palabra "material" utilizada con cada uno de estos componentes o riesgos, se refiere a un error que debe considerarse significativo cuando se lleva a cabo una auditoría. En una auditoría aplicada aun sistema en desarrollo, la definición de riesgos materiales depende del tamaño o importancia del ente auditado así como de otros factores. El auditor de sistemas debe tener una comprensión de estos riesgos de auditoría al planificar. Una auditoría tal vez no detecte cada uno de los potenciales errores en un universo. Pero, si el tamaño de la muestra es lo suficientemente grande, o se utiliza procedimientos estadísticos adecuados se llega a minimizar la probabilidad del riesgo de detección. De manera similar al

evaluar los controles internos, el auditor al evaluar un sistema en desarrollo debe percibir que en un sistema dado se puede detectar un error mínimo, pero ese error combinado con otros, puede convertiré en un error material para todo el sistema. La materialidad en la auditoría de sistemas debe ser considerada en términos del impacto potencial total para el ente en lugar de alguna medida basado en lo monetario.

Utilizando los componentes de los Sistemas de Información se deben cualificar los controles actuales y variaciones relacionadas con el componente. Para dichos valores es necesario determinar su participación porcentual con respecto al total. También se puede utilizar información presupuestal y valores de mercado.

La materialidad se califica entre 1 y 5 tal como se muestra a continuación:

Tabla No 4: Cuadro de grado de materialidad de los riesgos

GRADO DE MATERIALIDAD	CALIFICACIÓN	CONDICION
Insignificante La pérdida es baja	1	No hay datos o perjuicios
Bajo La pérdida es media	2	Se puede subsanar los daños inmediatamente

Medio La pérdida es alta	3	Se necesita asistencia de un tercero para subsanar los daños
Grave Perdida parcial	4	Daños extensivos, pérdida de la capacidad de operación que no tiene efectos perjudiciales.
Muy grave Pérdida total	5	Pérdida de la capacidad de operación que tiene efectos perjudiciales.

3.4.5. La probabilidad de ocurrencia del riesgo.

Obtenida básicamente del conocimiento, experiencia, resultados de intervenciones anteriores, estadísticas existentes, etc.

La probabilidad de ocurrencia del riesgo se califica cuantitativamente con los siguientes grados:

Tabla No 5: Cuadro de grado de probabilidad de riesgos

GRADO DE PROBABILIDAD	CALIFICACION	CONDICION
Improbable	1	El evento ocurriría solamente en circunstancias excepcionales.
Remoto	2	El evento podría ocurrir en algún momento y se considera que es difícil que suceda
Factible	3	El evento puede suceder eventualmente
Probable	4	El evento probablemente ocurriría
Muy probable	5	Se espera que el evento ocurra en la mayoría de los casos

Tabla No 6: Cuadro de relación de materialidad/probabilidad de ocurrencia

MATERIALIDAD/ PROBABILIDAD DE OCURRENCIA	INSIGNIFICA. 1	BAJO 2	MEDIO 3	GRAVE 4	MUY GRAVE 5
Muy probable 5	5	10	15	20	25
Probable 4	4	8	12	16	20
Moderado 3	3	6	9	12	15
Remoto 2	2	4	6	8	10
Improbable 1	1	2	3	4	5

	Riesgo insignificante
	Riesgo bajo
	Riesgo moderado
	Riesgo alto

DESPACHO DE AUDITORIA EN DESARROLLO 2007, S.A. DE C.V.

MATRIZ DE RIESGO DEL SISTEMA SAP DE LA ENTIDAD-ISSS

Nº	COMPONENTE	SUB COMPONENTE	DESCRIPSION DE RIESGOS	IMPACTO POR LA OCURRENCIA	CALIFICACION DEL IMPACTO MATERIAL	CAUSAS DEL RIESGO	CONTROL ASOCIADO	PROBABILIDAD DE OCURRENCIA	CALIFICACION DEL RIESGO
1			No proporcionar informacion suficiente apropiada	Retraso en la entrega de la informacion sistematizada	Grave	inconsistencia en la conciliacion de cifras y falta de oportunidad de la informacion	Conciliacion y comparaciones mensuales	Remoto	Moderado
			Interfaz de usuarios	Administración de datos erronea		Falta de claridad en los precedimientos para el registro de las operaciones del programa	Aplicación de procedimientos para el registro de las operaciones del programa		
			Administracion de cambios de red	Mala distribución del equipo		retraso o no inclusión de los ajustes solicitados por parte del programa			
			Origen de Datos: inexistencia de espacios para correcciones y firmas de usuario funcional y tecnico	Afectaria los resultados en el uso de los datos para los Usuarios Estrategicos, incumpliendo el objetivo de oportunidad en la entrega de información	Medio	Retrasos en la transmisión de información al personal usuario	Definir procesos claros en la generación y entrega de información	Moderado	Moderado
			Entrada de datos: actualización o desface en la entrada de datos, formatos no predefinidos			Retrasos en la transmisión de información al personal usuario	Establecer procesos de asistencia técnica para apoyar la generación de información		
			Procesamiento de datos: bajas de corriente, esto ocasiona caidas del sism tema			La estructura de cableado donde se esta desarrollando el sistema tiene falla en los enlaces satelitales	Falta de orgacionacion y comunicación entre las gerencias y los encargados del mantenimiento		
			Salida de información: reportes con fallas al momento de imprimir			Problemas con las bases técnicas al momento de elaborarlas por el consultor y esto ocasiona retraso en los programadores	Reglamentar los plazos maximos aceptables para la entrega de la informacion a los usuarios de las mismas		
			Back up: no existe seguridad de mantener archivos en red, ya que accidentalmente se pueden borrar	Perdida de inforamción por no realizar periodicamente back up	Muy Grave	Para guardar copias de la documetación que esta en red, no se cuenta con un plan de emergencias cuando surgen contingencias fuera de alcanze	Anticiparse a los cambios, con politicas claras y mantener un banco de la base de datos actualizada diariamente	Probable	Alto
			Lugares de resguardo: cuando ocurren accidentes fortuitos por ejemplo lluvia, el sistema se cae	afecta ya que no se tiene la información procesada en el momento que se necesita para la toma de		El personal funcional o usuarios no cuentan con ups apropiados para solventar estas situaciones	Asignacion de fechsa de resguardo de la información procesada por áreas		

DESPACHO DE AUDITORIA EN DESARROLLO 2007, S.A. DE C.V.

MATRIZ DE RIESGO DEL SISTEMA SAP DE LA ENTIDAD-ISSS

Nº	COMPONENTE	SUB COMPONENTE	DESCRIPCION DE RIESGOS	IMPACTO POR LA OCURRENCIA	CALFIACION DEL IMPACTO MATERIAL	CAUSAS DEL RIESGO	CONTROL ASOCADO	PROBABILIDAD DE OCURRENCIA	CALFICACION DEL RIESGO
1	[redacted]	[redacted]	Panorama Fisico: desastres naturales, acceso al centro de computo y niveles de alto voltaje	Deficiencia en los niveles de seguridad de las instalaciones	Muy Grave	Poca claridad en las responsabilidades para el manejo de la información	proporcionar mantenimiento a las areas donde estan instaladas los equipos	Moderado	Alto
			Panorama Tecnico: Lenguaje de programacion, fuentes o ejecutables de la instalacion	No conocer el sistema, puede ocasionar problemas en el momento de ocnfigurar		falta de conocimiento por parte de consultores al momento de efectuar consultas	Verificación selectiva del procedimiento de las tecnicas de control		
			Panorama Lógico: Virus informaticos, acceso no autorizado a bases de datos	Perdida de información		Infraestructura deficiente para el manejo de la red	Instalación de software de antivirus en cada terminal con su respectiva licencia		
			Valores parametrizables del sistema: falta de autorizacion de personal a parametrizar el sistema y restricciones al acceso de parametrización	Desgaste del personal encargado, ya que hay pocos recursos asignados		Procedimientos lentos al efectuar la parametrizacion	Aplicación de los procedimientos para la parametrizar los valores		
			Pistas de Auditoria: En la red de esta la bitacora diaria, pero no lo actualizan en su momento.	Duplicidad de tareas		Procedimientos deficientes para la consulta de bitacoras	Actualización de bitacoras para monitorear las bases de datos de los		
3	[redacted]	[redacted]	Carencia de Controles Administrativos: mala planificación organizacional y monitoreo	Que los procesos y desarrollos de los manuales no esten terminados al momento de ejecutar pruebas integrales del sistema.	Muy Grave	Retraso en revision de manuales, normas y los procedimientos por parte de las jefaturas o tambien cambios significativos en los procesos	Se atiende oportunamente los requerimientos de las jefaturas y se corrigen oportunamente.	Moderado	Alto
4	[redacted]	[redacted]	Capacidad: Mala planificacion de la capacitación	Mala operatividad de los usuarios al sistema y resitencia al cambio.	Muy Grave	Falta de compromiso de las jefaturas y comunicación con la encargada de impartir la capacitación	Monitorear por centro de atención al personal idoneo para recibir la capacitación	Moderado	Moderado

3.5. ALCANCE.

Las partes que se van a evaluar en la auditoria en desarrollo se detallan a continuación dividen en:

3.5.1. Análisis, diseño y programación.

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.

Por tanto, es necesario enfatizar que la evaluación de las diferentes etapas tiene un objetivo específico a perseguir por lo que se definen a continuación:

a) **Etapa de análisis:**

   Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.

b) **Etapa de diseño:**

   Errores, debilidades, omisiones antes de iniciar la codificación.

c) **Etapa de programación:**

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

Esta actividad es muy importante ya que el costo de corregir errores es directamente proporcional al momento que se detectan:

a) Si se descubren en el momento de programación será más alto que si se detecta en la etapa de aplicaciones de los sistemas de información,
b) Busca comprobar que la aplicación cumple las especificaciones del usuario,
c) Que se haya desarrollado dentro de lo presupuestado,
d) Que tenga los controles necesarios y que efectivamente cumpla con los objetivos y beneficios esperados.

Figura No 3: Organigrama de programa de auditoria en las etapas de análisis y diseño.

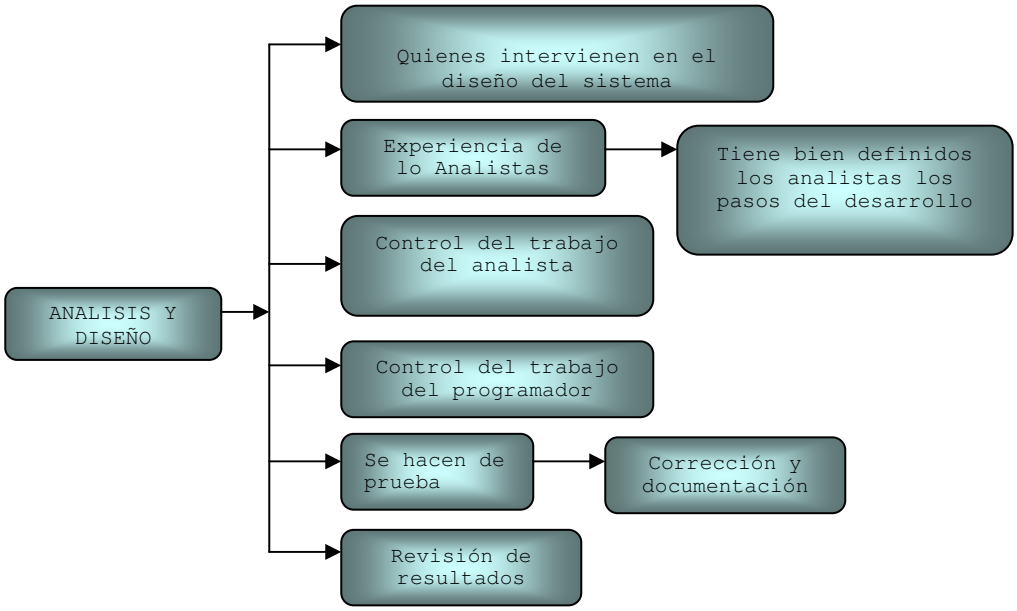
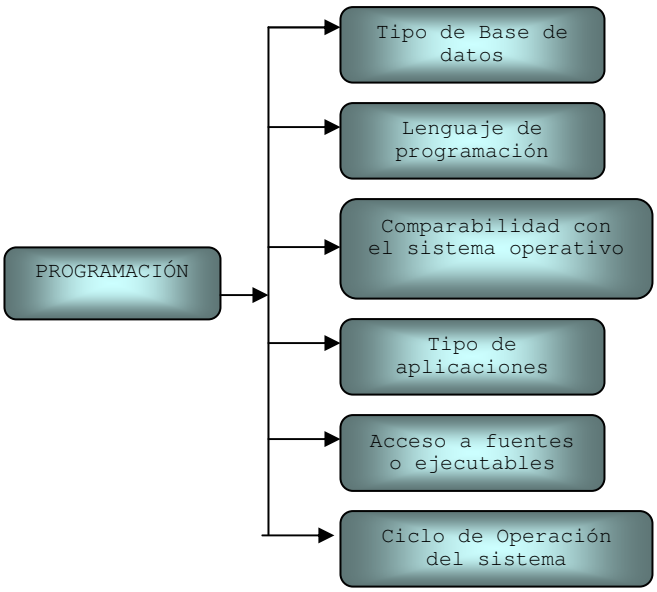


Figura No 4: Organigrama de programa de auditoria en la etapa de programación.



3.5.2. Prueba modular e integral.

En esta parte se trata de evaluar de forma integral el sistema SAP que se encuentra en la fase de desarrollo por lo que se considera necesario tomar en cuentas lo siguiente:

3.5.2.1. Percepción de usuarios

En esta parte hay que analizar los diferentes usuarios que son:

a) **Usuarios directos:**

Son aquellos que tendrán el acceso al sistema en todas las áreas relacionados al perfil de trabajo que realiza.

b) **Usuarios indirectos:**

Son aquellos que se les da acceso solo al modulo que el manejará.

Los aspectos más importantes a evaluar en esta parte es:

a) Identifique cuales son los usuarios directos e indirectos.
b) Conozca la percepción que tiene el usuario directo del Sistema.

El usuario del sistema evaluará si se puede emitir diferente documentación que ayude a la toma de decisiones a la administración; entre los reportes que se pueden emitir, se encuentran los siguientes:

i. Saldos diarios de una cuenta de gastos (binder).
ii. Acumulado de saldos desde la apertura del ejercicio a la fecha.
iii. Sistema esta integrado con los módulos antes mencionados.
iv. Catálogo actualizado.
v. Listado de cuentas por cobrar

vi. Listado de cuentas por pagar, con saldos de 30, 60, 90 días o más.
vii. Saldos de bancos para su respectiva conciliación.
viii. Reporte de saldos de balance de comprobación al mes que se le asigne que reportara.
ix. Consolidado mensual de las cuentas de mayor o subcuentas.
x. Listado de empleados con código y departamento o área a que pertenecen.
xi. Reportes de planillas de AFPS, clasificándolas a cual pertenecen cada uno de los empleados.
xii. Reporte de planillas de acuerdo al proyecto que se esta ejecutando según código asignado.

3.5.2.2. Funcionamiento del sistema.

El funcionamiento se puede verificar en:

a) **Origen de datos**:

Con relación al origen de datos documental, el sistema para que emita información debe de retroalimentarse por medio de partidas manuales y este consolida la información y al imprimir cualquier reporte requerido esto ya viene en el formato diseñado; es decir, con la siguiente información:

i. Fecha de ingreso
ii. Concepto
iii. Que tipo de movimiento es (diario, Ingreso y egreso)
iv. El código asignado según catalogo para elaborar la partida
v. El correlativo del movimiento del día
vi. Le índica además si quiere imprimir la partida al momento o hasta que este completamente segura.

b) **Entrada de datos**

En el ingreso o registro de datos al sistema es muy amigable, ya que permite al momento de ingresar datos poder verlos previamente antes de imprimirlos y así validar si esta según el soporte legal que lo documente.

El sistema tiene distintos campos para poder ingresar a cada modulo o también opciones que nos va facilitando la operatividad del sistema.

c) **Salida de información:**

El sistema permite emitir distintos reportes según la necesidad de cada usuario, siendo de vital importancia para la administración, por ejemplo:

Si emite un reporte dependiendo del módulo solicitado y este tendrá las interfaces respectivas para que la información solicitada sea la adecuada.

Al momento de imprimir los reportes el sistema es capaz de ordenarlos automáticamente, con el objetivo de que no se repita ningún documento.

3.5.2.3. Niveles de seguridad del sistema.

Los niveles de seguridad se pueden verificar en:

a) **Panorama físico:**

El panorama físico es un factor de suma importancia en la institución, y principalmente en el lugar donde esta instalada la red. Esta consideración debemos de reflejar más que todo en las políticas que tiene la institución para el área de sistemas ya que tenemos que considerar ciertos elementos para la seguridad física de la información entre los cuales tenemos:

i. La ubicación del procesador,

ii. Materiales utilizados para su construcción,

iii. Equipo de detectores y protección contra incendios,

iv. Sistema de aire acondicionado,

v. Instalación eléctrica,

vi. Seguridad en el acceso del personal

vii. Elaborar backups

viii. Sistema de control de acceso y el entrenamiento al personal u operadores.

ix. Todo el entorno del ambiente en si.

b) ***Panorama lógico***

Guía de entrevista al jefe del departamento informática

i. Nombre del puesto del entrevistado

ii. Puesto del jefe inmediato

iii. Puestos y números de personas que le reportan al entrevistado

iv. Están debidamente delimitadas las responsabilidades de cada empleado

v. Describa brevemente las actividades diarias de su puesto

vi. Actividades periódicas.

vii. Actividades eventuales.

viii. ¿Con que manuales cuenta para el desempeño de las labores de los analistas, programadores y personal de apoyo?

ix. Mencione los objetivos generales y específicos enfocados al área de informática al desarrollo del sistema.

x. ¿Como reciben las instrucciones de los trabajos encomendados?

xi. ¿Con que frecuencia reciben capacitaciones los empleados?

xii. Las políticas se encuentran actualizadas en todas las actividades y son del conocimiento del personal

c) ***Del procesamiento de datos y de los equipos de computo***

i. Conocen los empleados el modelo relacional del sistema computarizado.

ii. ¿Cubre las necesidades el sistema que se esta desarrollando?

iii. ¿Quien interviene en el diseño del sistema?

iv. ¿Existen normas que definan el contenido de los instructivos de captación de datos?

v. ¿Quién y como controla las entradas de la información de documentos fuente?

vi. Se verifica la calidad de la información recibida para el procesamiento de datos.

vii. ¿Existen fallas de exactitud en los procesamientos de información?

viii. Mantienen un registro de anomalías del procesamiento de la información.

ix. Existen órdenes de proceso para cada corrida en computadora.

x. Le han realizado actualizaciones últimamente al software.

xi. Utilizan un manual de control interno a las bases de datos.

d) **Oportunidad de información para los *usuarios:***

El proceso de información es muy factible ya que el sistema es muy amigable, en la pantalla le menciona las opciones y con solo darle opción asignada el mismo sistema lo guía a elaborar lo que el usuario quiere.

El proceso para registrar un mes es sencillo, ya que se ingresa toda la información necesaria y luego tiene la opción para cerrar el mes con su año correspondiente es de tomar en cuenta si usted tiene cerrado el mes siguiente no le permite el sistema cerrar tiene que seguir lineamiento lógico del sistema.

La salida de información es muy accesible ya que el sistema le da opciones donde solo al asignarle el numero que el usuario le asigne, así le reportara la información requerida.

e) ***Panorama técnico:***

Dentro de la estructura de la organización se debe comprobar si existe una función para la administración y control de la seguridad de acceso a los datos, un responsable de seguridad que sea independiente del área de Sistemas de Información y que se reporte al máximo nivel de autoridad.

En el sistema en desarrollo actualmente no existen políticas para la seguridad informática, en la que se detallen como mínimo los siguientes aspectos:

i. Nivel de confidencialidad de los datos

ii. Procedimiento de otorgamiento de claves de usuarios para el ingreso a los sistemas

iii. Estándares fijados para el acceso de usuarios.

iv. Monitoreo de claves y accesos autorizados para cada usuario

v. Existencia de bloqueos para usuarios al ingresar a Internet en páginas que no tengan relación a la actividad de la institución.

vi. Para ingresar al sistema cada usuario de acuerdo al perfil autorizado tendrá su clave o password, para brindar mayor seguridad a las áreas donde están detallados las actividades que este realizara.

También es importante mencionar que al ingresar al sistema el usuario solo tiene 3 oportunidades para ingresar el password si en la tercera no se recuerda el sistema le bloquea el acceso.
El sistema en desarrollo no puede ser manipulado por usuarios que no estén autorizados, ya que los cambios de usuario solo lo puede realizar el encargado en la servidora y no todos tienen acceso a esta maquina.

f) **Valores parametrizables del sistema:**

El sistema en desarrollo tiene en los valores parametrizables es muy especifico en el detalle de cada uno de los accesos restringidos para los usuarios. Cada modulo tiene los accesos restringidos solo se autoriza el que realmente va a operar.

En el sistema cada modulo tiene específicamente los lineamientos a seguir y le va pidiendo la información según el avance por ejemplo una partida de ingreso debe, haber, si no el sistema le indica que no esta cuadrada.

g) ***Pistas de auditoría (Bitácora de registro de eventos):***

En el sistema en desarrollo deben existir controles para el ingreso, son los siguientes:

a- Solo se puede ingresar al modulo tres veces, si por un caso se le olvido la contraseña el sistema lo bloquea

b- Los accesos son restringidos al sistema, solo el usuario de acuerdo al perfil autorizado podrá ingresar.

h) **Backup:**

En la institución tiene como política realizar backup diariamente del sistema con los datos ya incorporados.

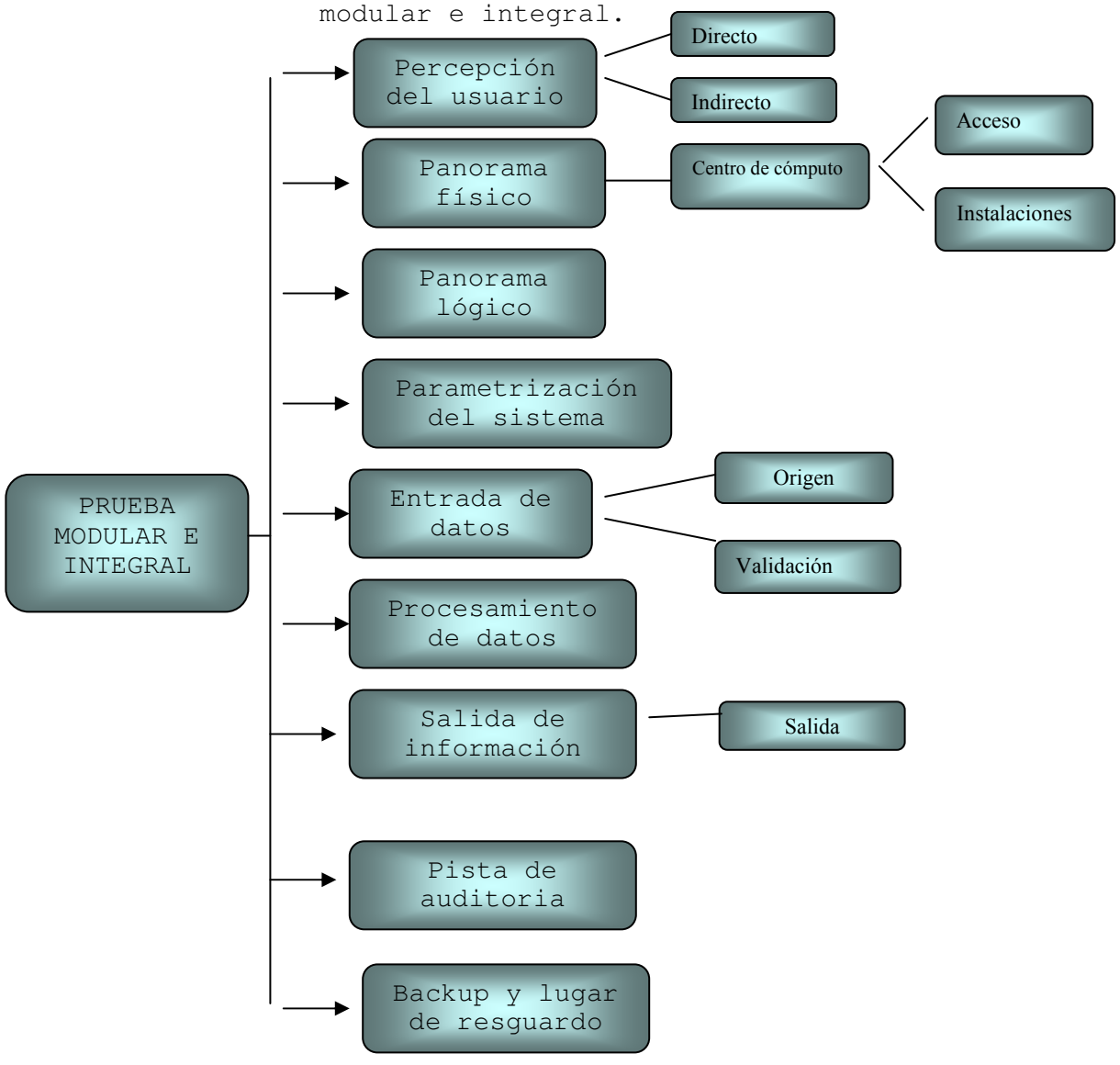
También se realiza una copia de respaldo en cada disco duro de la maquina, esto normalmente es realizada cada dos días, esta

copia la realiza cada usuario para resguardarse del trabajo realizado.

i) **Lugares de resguardo:**

Las copias que se realizan las guarda el responsable asignado por la unidad de informática, con el objetivo de resguardar la información de toda la institución por algún desastre natural.

Figura No 5: organigrama de programa de auditoria en la prueba modular e integral.



3.5.3. Desarrollo de manuales.

Al desarrollar un sistema los encargados deberán tener en cuenta los procesos y normas que se establecen al momento de desarrollar el sistema ya que deberá estar detallado lo más claro posible para que el usuario final lo comprenda y sea factible al momento de la capacitación.

a) **Procedimientos.**

i. Reglamento interno de la institución donde se detalla las obligaciones del empleado como del patrono y sus beneficios.

ii. Normativa existente en la institución para regirse por ella y acatar su uso.

b) **Marco legal.**

i. **Leyes mercantiles**

Ley de propiedad Intelectual.

Decreto Legislativo Nº. 799, del 2 de febrero de 1994, publicado en el D.O. Nº. 56, Tomo 322, del 21 de marzo de 1994.

Última reforma:

D. L. 985, del 17 de marzo de 2006, publicado en el D.O. No. 58, Tomo 370 del 23 de marzo de 2006.

ii. **Leyes tributarias**

Código tributario

Decreto Legislativo N°. 230, del 14 de diciembre de 2000, publicado en el D.O. N°. 241, tomo 349, del 22 de diciembre de 2000.

Última reforma:

Decreto Legislativo N°. 730, del 29 de Junio del 2005, publicado en el D.O. N°. 127, Tomo 368, del 08 de Julio del 2005 final del formulario

Reglamento del código tributario

Decreto Legislativo No. 230, de fecha 14 de diciembre de 2000, publicado en el Diario Oficial No. 241, Tomo 349, del 22 de ese mismo mes y año se emitió el Código Tributario.

Ley de impuesto sobre la Renta

Decreto Legislativo número 472 de fecha 19 de diciembre de 1963, publicado en el Diario Oficial N°. 241, Tomo 201 del 21 del mismo mes y año

Última reforma:

Decreto Legislativo N°. 182, del 14 de Diciembre del 2006, publicado en el D.O. N°. 4, Tomo 374, del 8 de Enero del 2007.

Reglamento de la ley de impuesto sobre la Renta

Decreto Legislativo N°. 134, de fecha 18 de diciembre de 1991, publicado en el Diario Oficial N°. 242, Tomo 313 del 21 del mismo mes y año.

Última reforma:

Decreto Legislativo N°. 117, del 11 de diciembre del 2001, publicado en el D.O. N° 234, Tomo 353, del 11 de diciembre del 2001.

Ley SAFI (ley de administración Financiera Institucional)

Ley de impuesto a la transferencia de bienes muebles y a la prestación de servicio.

Decreto Legislativo N°. 296, del 24 de julio de 1992, publicado en el D.O. N°. 143, Tomo 316, del 31 de julio de 1992.

Última Reforma:

Decreto Legislativo N° 644, del 17 de marzo del 2005, publicado en el D.O. N° 55, Tomo 366, del 18 marzo del 2005.

Reglamento a la ley de impuesto a la transferencia de bienes muebles y a la prestación de servicio.

Decreto Legislativo número 296 de fecha 24 de julio de 1992, publicado en el Diario Oficial N°. 143 Tomo 316 del 31 del mismo mes y año

Última Reforma:

Decreto Legislativo N° 117, del 11 de diciembre del 2001, publicado en el D.O. N° 234, Tomo 353, del 11 de diciembre del 2001

Ley del registro a la Importación.–

Decreto Legislativo. N° 224, del 14 de diciembre de 2000, publicado en el D.O. N° 241, tomo 349, del 22 de diciembre de 2000.

Última Reforma:

Decreto Legislativo N° 551, del 20 de septiembre de 2001, publicado en el D.O. N° 204, tomo 353, del 29 de octubre de 2001.

Ley de adquisiciones y contrataciones de la administración pública.

D.L. N° 868, del 5 de abril del 2000, publicado en el D.O. N° 88, Tomo 347, del 15 de mayo del 2000.

Últimas Reforma:

D.L. Nº. 909, del 14 de diciembre del 2005, publicado en el D.O. Nº. 8, Tomo 370, del 12 de enero del 2006.

iii. **Leyes Civiles / Laborales**

Código civil

La Cámara de Senadores ordenó la redacción del Código Civil por decreto de 4 de febrero de 1858, comisionando al Poder Ejecutivo para nombrar la Comisión respectiva, para revisar el proyecto que se elaborará y para darle fuerza de ley; la Cámara de Diputados aprobó tal decreto el día 12 siguiente y el Poder Ejecutivo lo sancionó mediante decreto Nº. 7 del Ministerio General de fecha 13 del mismo mes y año, según consta de la Gaceta de El Salvador del 17 de febrero de 1858.

Última Reforma:

D.L. Nº 512, del 11 de noviembre del 2004, publicado en el D.O. Nº 236, Tomo 365, del 17 de diciembre del 2004.

Código de trabajo

D.L. Nº. 15, del 23 de junio de 1972, publicado en el D.O. Nº. 142, Tomo 236, del 31 de julio de 1972.

Últimas reforma:

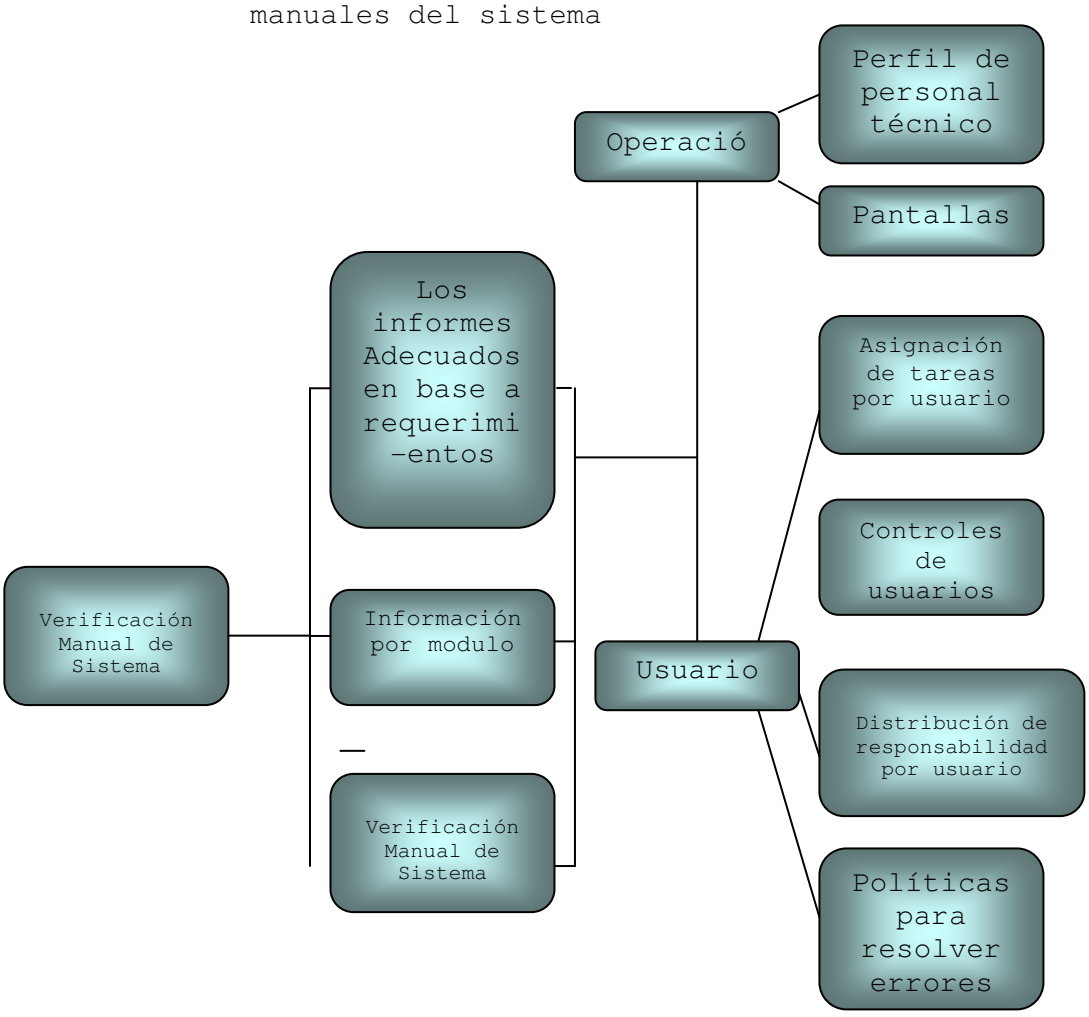
D.L. Nº. 611, del 16 de febrero del 2005, publicado en el D.O. Nº. 55, Tomo 366, del 18 de marzo del 2005.

Contrato Colectivo de trabajo vigente

San Salvador, uno de febrero de dos mil cinco.

Vigencia desde 2005-2008, mayo 2005

Figura No 6: Organigrama de programa de auditoria en la etapa de manuales del sistema



3.5.4. Entrenamiento (capacitaciones).

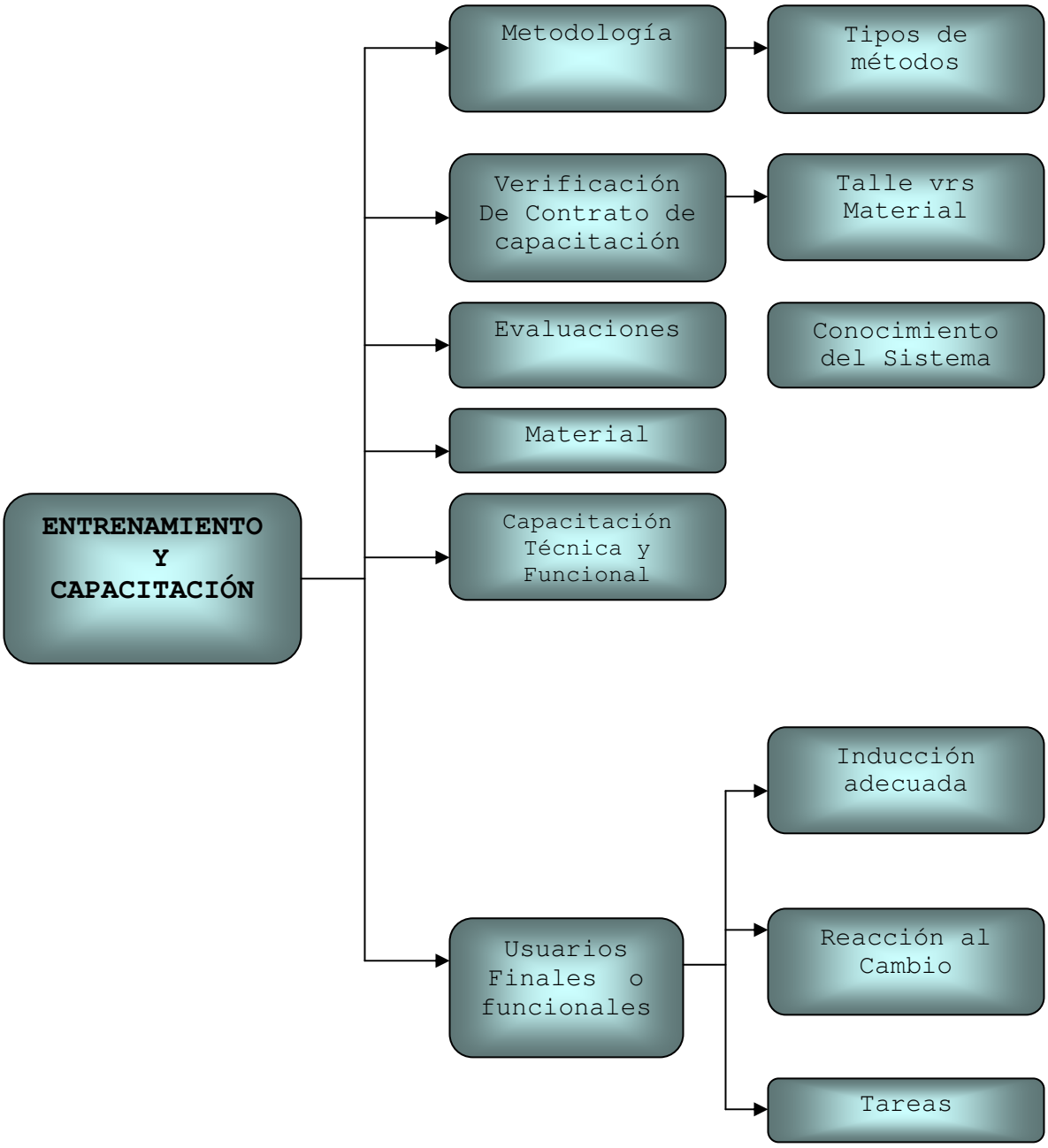
Al momento de finalizar el desarrollo del sistema los responsables asignados para las capacitaciones tanto a los

usuarios funcionales y finales deberá de existir una planificación adecuada en todos los centros médicos/hospitalarios donde se desarrollara la prueba piloto y se implementara el sistema.

Para implementar un sistema debe existir una concientización y sensibilidad de los usuarios, ya que hoy en día los usuarios se resisten al cambio; ya que creen que serán sustituidos por personal adecuado e idóneo.

Es por ello que antes de terminar el desarrollo del sistema debe de existir una capacitación antes de implementarlo, para que el usuario tenga conocimiento y se de cuenta de la herramienta útil que tendrán a su disposición.

Figura No 7: Organigrama de programa de auditoria en la etapa de entrenamiento y capacitación.



3.6. ADMINISTRACION DEL TRABAJO.

3.6.1. Personal de auditoría.

La asignación del personal se determinará en función de las programaciones semanales que elabore Supervisión, previa aprobación por la gerencia de auditoría.

Seleccionamos del cuerpo de profesionales de la Firma, las personas que mejor encajan a los requerimientos técnicos y operativos de esta auditoría; El trabajo completo se desarrollará con las personas siguientes:

Tabla No 8: Cuadro de personal asignado de auditoría

PERSONAL ASIGNADO	
Socio Director:	Licda. Maria Esmeralda Rivas
Supervisores:	Licda. Claudia Lorena Galdamez Licda. Maria José Polanco
Coordinadores:	Lic. José Renato García Lic. Carlos Roberto Pascasio
Asistentes:	Lic. Remberto Hernandez Guardado Licda. María Alicia Renderos Licda. Patricia Esmeralda Ayala

3.6.2. Funciones específicas del personal asignado.

a) **Socio director**

Cuenta con una experiencia de más de doce años en el área financiera contable, fiscal y de Sistemas de información en

desarrollo y ejecutables, se ha desempeñado como Contador General, Auditor de sistemas, Contralor, Gerente Financiero de instituciones de sólido prestigio con firmas internacional.

A nivel académico posee Lic. En Contaduría Pública y Maestría en Administración Financiera

Un sumario de los deberes y responsabilidades por categoría jerárquica, es el siguiente:

Tiene la responsabilidad primaria y absoluta de asegurar que el examen sea efectuado de conformidad con las Normas de Auditoría de Sistemas, Normas Internacionales de Auditoría, Leyes y Regulaciones Aplicables.

Tiene la obligación de velar que se proporcionen a la Compañía todos los servicios que necesite de la Firma. Sus deberes incluyen muchas consideraciones y por tal motivo la siguiente lista no pretende ser exhaustiva:

i. Mantener la relación primaria con el personal ejecutivo respectivo del cliente.

ii. Aprobar el alcance general de la revisión.

iii. Dirigir y autorizar los Planes de Trabajo y los Programas de Auditoría.

iv. Participar y resolver todos los aspectos técnicos de Contabilidad y Auditoría relativos al trabajo contratado.

v. Revisar memorandos, papeles de trabajo y otra información preparada y obtenida en relación con nuestro examen.

vi. Establecer la naturaleza y contenido de los Informes de Auditoría, y aprobarlos antes de que sean emitidos.

b) **Supervisor**

Cuenta con 8 años de experiencia en el área de Auditoría de Sistemas, con capacidades eficientes y aptitudes necesarias para desempeñar el cargo en el área asignada.

Su función será verificar la calidad del trabajo, con base en las Normas Internacionales de Auditoría y de sistemas a fin de constatar que el trabajo se desarrolle con apego a la presente oferta de servicios y el contrato de servicios de auditoría que se suscriba, y demás normativa y legislación aplicable; entre sus actividades destacan las siguientes:

vii. Verificar que el alcance de la planeación y los programas de auditoría, estén diseñado de tal forma que permitan el logro satisfactorio de los objetivos del examen.

viii. Supervisar durante el desarrollo y ejecución de la auditoría, el trabajo de los miembros del personal responsable, para constatar que las labores se están desarrollando tal como fueron planeadas y tomar las medidas correctivas, si fuere necesario.

ix. Verificar que el contenido de los informes esté documentado con evidencia suficiente, competente y relevante en los papeles de trabajo.

x. Las conclusiones en el informe sean lógicas y fluyan de los hallazgos de auditoría.

xi. Que las recomendaciones sean factibles y dirigidas a corregir la condición y la causa del hallazgo.

xii. Evaluar si el informe cumple con las Normas Internacionales de Auditoría.

xiii. Determinar que cada objetivo del trabajo haya sido cubierto, y que los hallazgos se relacionen con dichos objetivos.

xiv. Verificar que las conclusiones sobre declaraciones, números y montos estén documentados en los papeles de trabajo.

xv. Registrar sus observaciones en las hojas de trabajo y verificar que hayan sido atendidas por el grupo de auditoría a satisfacción del Socio Director.

xvi. Archivar adecuadamente su revisión en los papeles de trabajo junto con el borrador del informe, y a la disposición para cualquier revisión de control de calidad.

xvii. Referenciar en forma independiente los informes de auditoría, antes que sea terminados y emitidos. Las Normas de Auditoría requieren que el borrador del informe cuente con un índice y referencias cruzadas adecuadamente.

xviii. Reportar directamente con el Socio Director los resultados de su trabajo.

xix. En general, será el encargado de darle seguimiento de las diferentes actividades que realice el personal responsable de la auditoría, para asegurarse la calidad del trabajo.

c) **Coordinador:**

Cuenta con 6 años de experiencia en el área de Sistemas de Información y fiscal, sus estudios son Lic. en Contaduría Publica y capacitaciones en programaciones de sistemas.

Será el profesional a cargo del trabajo que dedicará mayor tiempo, sus deberes y responsabilidades serán las siguientes:

i. Confirmar con el Supervisor, mediante los Programas y reuniones, el Alcance que se le va a dar al trabajo.

ii. Discutir con el Supervisor lo relativo a las asignaciones de trabajo.

iii. Controlar el tiempo empleado en el trabajo.

iv. Desarrollar los procedimientos de Auditoría necesarios para completar el trabajo, especialmente en las áreas difíciles.

v. Comunicar los problemas inmediatamente y mantenerlo informado del progreso, así como de las irregularidades que considere importantes.

vi. Hacer los arreglos, cuando sea necesario, para comentar y resolver los problemas con el Cliente.

vii. Asegurarse que se han cubierto todos los puntos en el Programa.

viii. Asegurarse de que todos los papeles de trabajo estén completos.

ix. Asegurarse de que todos los puntos pendientes han sido resueltos satisfactoriamente.

x. Asegurarse de que los memos de revisión de los Asistentes estén terminados.

xi. Asegurarse de que las confirmaciones fueron recibidas y cotejadas, y las diferencias fueron aclaradas.

xii. Asegurarse que se ha obtenido la carta de salvaguarda.

d) **Asistentes:**

Cuentan con 5 años de experiencia en el área de Auditoría de Sistemas de informaron en desarrollo y ejecutables.

Desarrollarán las funciones siguientes:

i. Elaborar papeles de trabajo.

ii. Comprobación muestral o aleatoria de asientos o partidas.

iii. Verificación de cálculos aritméticos.

iv. Revisión de procedimientos de las bases de datos.

v. Validación de la integridad de los datos.

vi. Evaluación del sistema de información.

vii. Todas aquellas asignadas por el Coordinador.

3.7. PERSONAL AUDITADO.

Tabla No 9: Cuadro de personal auditado y sus funciones generales

CARGO	FUNCIÓN GENERAL DEL PUESTO
Gerente de división de informática	Monitorear el sistema
Jefe de mantenimiento de sistemas	Verificar que el sistema funcione adecuadamente

Jefe Operativo de sistemas	Verificar que los sistemas operativos no tengan dificultades
Jefe de Tecnología	Verificar que el sistema y equipo funcione adecuadamente.
Técnico	Reparación y mantenimiento a las base de datos y equipo
Técnico	Reparación y mantenimiento a las base de datos y equipo

Los reportes los entregaran los encargados de la operativización del sistema, entre los que podemos mencionar:

3.7.1. Gerente de informática

Es el responsable de la información solicitada por el auditor de la Base de Datos, para la realización de pruebas de validación de la integridad de los datos, nos proporcionara el Código Fuente o su funcionamiento.

Y autorizará a los empleados a su cargo de proporcionar la información pertinente para evidencia de auditoría.

3.7.2. Jefe de mantenimiento de sistemas

Es responsable de los controles detectivos, preventivos y correctivos del funcionamiento de los equipos informáticos, desde el momento de la entrada, procesamiento y salida de la información.

Proporcionara las normativas aplicables al sistema y entorno de aplicación y los manuales técnicos y aplicaciones del usuario.

3.7.3. Jefe operativo de sistemas.

Es el responsable de la seguridad, administrador de las redes, eficiencia e integridad de los datos generados dentro del sistema de Información.
Proporcionara la estructura de las redes, las relaciones existentes entre los módulos de aplicatividad del Sistema, como los diferentes niveles de seguridad.

3.7.4. Técnicos.

Son los responsables del registro de los datos y mantenimientos adecuados al área para que los equipos estén en óptimo condiciones.
Proporcionara toda la información que sea necesario en el transcurso de la auditoría. Una computadora para poder realizar las TAAC.

3.8. RESUMEN DEL TRABAJO.

Los servicios de auditoría que prestaremos a la institución se definen a continuación:

3.8.1. Fechas Claves y actividades principales.

Las Fechas claves en la auditoria a desarrollar son:

a) 15 días después de iniciado el proceso de evaluación de los riesgos asociados al sistema, se presentara la carta de gerencia: Periodo Septiembre 2007.
b) Elaboración de los papeles de trabajo, considerando la realización de los Programas de Auditoría: Periodo Septiembre/ 2007.

3.8.2. Informe a emitir.

Con base en los resultados obtenidos en la evaluación del control interno de la institución y en la ejecución del trabajo de campo de la auditoría, se emitirán los siguientes reportes:

3.8.2.1. Carta de gerencia.

Contendrán las siguientes observaciones e irregularidades encontradas en el examen de cada área y su repercusión en el efectivo funcionamiento de las aplicaciones informáticas, cumplimiento con las normativas y requisitos legales establecidos para la actividad, integridad de los datos.

3.8.2.2. Informe de auditoría.

El informe final de servicios de auditoría del sistema en desarrollo correspondiente al período comprendido entre Agosto a Diciembre de 2006, será preparado de acuerdo a Normas auditoría de Sistemas y Normas Internacionales de Auditoría.

3.9. PRESUPUESTO DE RECURSOS.

3.9.1. Personal asignado, tiempo y costos.

Comprende el número de horas/ hombre estimados para desarrollar el trabajo por el personal técnico de la Firma.

El tiempo estimado para la ejecución de esta auditoría se detalla a continuación:

Tabla No 10: Cuadro de presupuesto de recursos

Cantidad	Categoría del personal	horas / hombre
1	Socio Director	9
2	Supervisor	19
2	Coordinador	30
3	Asistentes	92
Total Horas / hombre		**150**

El costo estimado para la ejecución de esta auditoría se detalla a continuación:

Tabla No 11: Cuadro de asignación de costos de auditoría

Cargo	Sueldo	Vacaciones	Aguinaldo	Indemnización	Aporte ISSS	Aporte AFP	Total	Costos indirectos	Total de costos	Horas hombre	Horas	Total oferta
Socio Director	$ 5,000.00	$ 267.12	$205.48	$ 55.98	$ 51.43	$ 337.50	$ 5,917.51	$ 1,183.50	$ 7,101.02	$ 29.50	9	$ 266.29
Supervisor	$ 3,000.00	$ 160.27	$123.49	$ 55.98	$ 51.43	$ 202.50	$ 3,593.47	$ 718.69	$ 4,312.17	$ 17.97	19	$ 341.38
Coordinador	$ 2,500.00	$ 133.56	$102.74	$ 55.98	$ 51.43	$ 168.75	$ 3,012.46	$ 602.49	$ 3,614.95	$ 15.06	30	$ 451.00
Asistentes	$ 600.00	$ 32.05	$ 24.66	$ 49.32	$ 45.00	$ 40.50	$ 791.53	$ 158.31	$ 949.83	$ 3.96	46	$ 182.05
Asistentes	$ 600.00	$ 32.05	$ 24.66	$ 49.32	$ 45.00	$ 40.50	$ 791.53	$ 158.31	$ 949.83	$ 3.96	46	$ 182.05
Sub total	**$ 11,700.00**	**$ 625.07**	**$480.82**	**$ 266.58**	**$ 244.28**	**$ 789.75**	**$ 14,106.50**	**$ 2,821.30**	**$ 16,927.80**	**$ 70.53**	**150**	**$ 1,423.64**
MARGEN DE UTILIDAD												**$ 427.09**
TOTAL GENERAL												**$ 1,850.73**

3.9.2. CRONOGRAMA DE ACTIVIDADES.

Tabla No 12: Cronograma de actividades de auditoría a realizar.

Tiempo / Tiempo Actividades	Ago-07				Sep-07			
	1	2	3	4	1	2	3	4
Planeación								
Memorando de planeación								
Alcance de auditoría								
Programas de auditoría								
Ejecución de programas de auditoría								
Carta de gerencia								
Informe de auditoría								
Conclusiones y recomendaciones								
Entrega de informe final								

3.10. EJECUCIÓN.

Una vez realizados los programas de auditoría, para el área específica, se procederá a efectuar cada actividad diseñada para lograr los objetivos de la auditoría obteniendo la evidencia suficiente y apropiada.

Realizada la planificación de la auditoría se prosigue a su ejecución, la cual estará determinada por las características concretas, los puntos y requerimientos que se estimaron en la planeación.

Una vez realizados los programas de auditoría, para el área específica, se procederá a efectuar cada actividad diseñada para lograr los objetivos de la auditoría obteniendo la evidencia suficiente y apropiada.

De acuerdo con el programa de auditoría, cada auditor tiene que realizar las actividades que corresponden conforme fueron diseñadas, en la cronología que le asignada a cada una, y respetando los tiempos y recursos que le corresponde utilizar, con el propósito de ejecutar los eventos programados y alcanzar el objetivo de la auditoría.

Conforme a la guía de auditoría se tienen que utilizar los instrumentos y herramientas elegidos para llevar a cabo la evaluación ya sea mediante recopilación y análisis de la información, observación, pruebas y simulaciones de los sistemas o cualquier otro diseñado previamente para tal efecto.

El auditor esta en la obligación de llevar un legajo donde se recopilen todos los papeles de trabajo que sustenten la evaluación y las observaciones reportadas.

Las hojas de trabajo deben elaborarse con los conceptos y cifras en el mismo orden que son presentados por los sistemas para

facilitar la presentación de los mismos o el cotejo de estos contra nuestros papeles de trabajo.

Por cada concepto, partida u operación principal del sistema debe existir una cédulas sumaria, en estas se deben relacionar las operaciones individuales del sistema que dan origen al conglomerado de los datos.

Generalmente hay una o varias cédulas de detalle para cada operación que es objeto de trabajo de auditoría, estas cédulas deben contener la evidencia de los análisis y pruebas efectuadas para formar una opinión sobre el funcionamiento del sistema, su desarrollo y la información que devuelve.

Si fuese necesario, se presentaran subcédulas para registrar pruebas de los datos que respaldan las operaciones del sistema o para desarrollar otros trabajos de auditoría necesarios.

3.11. INFORME DE AUDITORÍA.

Al finalizar el examen, se emitirá y remitirá un informe sobre la auditoría realizada; dicho informe serán discutidos con la gerencia general.

El informe final de servicios de auditoría en sistemas de información correspondiente al período comprendido entre Agosto y septiembre de 2007, será preparado de acuerdo a Normas Internacionales de Auditoría, además debe presentarse en forma clara, precisa y objetiva con los hechos reales debidamente sustentados, dando pautas al mejoramiento de los controles y seguridades establecidas dentro del sistema de información.

3.12. PROGRAMAS DE AUDITORÍA

La finalidad que persigue el auditor al realizarlas pruebas de cumplimiento es obtener evidencia de los controles internos necesarios para el logro de los objetivos específicos y que se están aplicando de forma continua en la manera que fueron prescritos.

3.12.1. Etapa 1: Programación

PROGRAMA DE AUDITORIA DE SISTEMAS INFORMATICOS EN DESARROLLO

Nombre de la entidad	:	Instituto Salvadoreño del Seguro Social
Fase auditada	:	Desarrollo de SAP
Actividad principal	:	Atención médico/hospitalaria

3.12.1.1. Objetivo general.

El objetivo es asegurarse de que el sistema funcione conforme a las especificaciones funcionales, a fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.

3.12.1.2. Objetivos específicos.

a) Identificar inexactitudes, ambigüedades y omisiones en las especificaciones.(etapa de Análisis)
b) Descubrir errores, debilidades, omisiones antes de iniciar la codificación. (Etapa de diseño)
c) Buscar la claridad, modularidad y verificar con base en las especificaciones. Etapa de Programación.

No.	Procedimiento	Hecho por	Ref.	Observaciones
1	Verifique si el lenguaje de programación en que se ha desarrollado la aplicación sea el compatible con el Sistema Operativo de la empresa.			
2	Mediante entrevista con el encargado de mantenimiento o soporte al sistema, verificar que lenguaje de programación y base de datos utiliza, específicamente los siguientes puntos: a) En que lenguaje de programación se ha desarrollado la aplicaron. b) Que base de datos se utiliza para almacenamiento de datos. c) Es una aplicación stand alone o cliente servidor d) Si es una aplicación cliente servidor, esta instalado localmente o por acceso remoto a base centralizada. e) La instalación contiene los fuentes o ejecutables f) Que control existe sobre las versiones distribuidas entre las dependencias usuarias			
3	Verifique la forma general en que opera el sistema, obtenga del técnico una descripción general de la forma en que la aplicación opera (ciclo de operación del sistema).			
4	Confirme si es una aplicación cliente servidor y si cumple con la instalación localmente o por acceso remoto a base descentralizada.			
5	Como se controla el trabajo de los programadores y analistas			
6	El Programador se coordinan con el analista y discuten el diseño y la programación en su conjunto			
7	Poseen diagrama de Bloques, tablas de decisiones			
8	Se revisa los resultados al correr el programa.			
9	Quienes realizan las correcciones de los programas.			
10	Compruebe si se cumple con el ciclo de operación del sistema.			

3.12.2. Etapa 2: Prueba modular e integral del sistema

PROGRAMA DE AUDITORIA DE SISTEMAS INFORMATICOS EN DESARROLLO

Nombre de la entidad	:	Instituto Salvadoreño del Seguro Social
Fase auditada	:	Desarrollo de SAP
Actividad principal	:	Atención médico/hospitalaria

3.12.2.1. Objetivo general.

Evaluar de forma integral el sistema SAP que se encuentra en la fase de desarrollo.

3.12.2.2. Objetivo específicos.

a) Evaluar los controles de calidad en acceso, procesamiento y salida de información.
b) orientados a mantener la integridad de los datos que ahí se almacenan.
c) Evaluar los controles y niveles de seguridad establecidos para el acceso *y uso de las aplicaciones informáticas.*

No.	Procedimiento	Hecho por	Ref.	Observaciones
	Percepción de Usuarios			
1	Identifique cuales son los usuarios Directos e indirectos			
2	Conozca la percepción que tiene el usuario directo del Sistema.			
	Panorama Físico			
3	Identifique el lugar de instalación de centro de cómputo de la empresa e identifique los procedimientos de acceso a estas, instalaciones de los usuarios externos e internos de la unidad de informática.			
4	Solicitar un listado del personal con acceso al centro de cómputo.			
5	Verifique el diseño del área del Centro de Cómputo, la existencia de alarma contra incendios, extintores, salida de emergencia señalizada.			
6	Verifique las paredes del lugar que no estén humedecidas ni agrietadas, no existan cables sueltos pertenecientes a la Red, tuberías de agua o fugas alrededor del área de ubicación del servidor, la existencia o falta de drenajes naturales o artificiales de agua.			
7	Verifique la existencia de aire acondicionados en el centro de cómputo, y que tipo de sistema es, la temperatura del aire acondicionado y nivel de humedad del centro de cómputo.			
8	Verifique la existencia de cableado de energía eléctrica encajuelados o subterráneos o están en forma visible.			
9	Verifique si tienen identificados los puntos de red en la empresa.			
10	Verifique la existencia de baterías de reguladores de voltaje en los equipos de computo tanto del servidor como del usuario			
11	Verifique si existe una planta de energía eléctrica auxiliar dentro de la institución.			
	Panorama Lógico			
12	Observe si cualquier usuario puede tener acceso fácilmente al sistema.			
13	Evalué el esquema de seguridad que se ha establecido para el acceso a las aplicaciones y a los datos que esta			

No.	Procedimiento	Hecho por	Ref.	Observaciones
	posee.			
14	Determine si existe un modulo especifico para la asignación de acceso a usuarios.			
15	Verifique cuales son las políticas que se aplican a la administración de la seguridad.			
16	Como se establecen los niveles de acceso a los usuarios. a) Identificación de usuario b) Password c) Mecanismos de autorización			
17	Evalué el nivel de protección existente sobre las tablas o base de datos de la aplicación: a) Verifique su alcance desde el DOS o desde Windows. b) Pruebe su acceso desde otros programas gestores de base de datos			
18	Verifique que se tengan instalados los archivos ejecutables de la aplicación y no los fuentes.			
19	Verifique que se tengan instalados los archivos de ejecución del software(rum time) y no el software completo.			
	Parametrización del sistema			
20	Verifique la existencia de alguna opción de parametrización del sistema, considerando lo siguiente: a) Quienes están autorizados a parametrizar el sistema. b) Como se restringe dicho acceso. c) Que elementos están parametrizados d) Verifique la forma en que se restringe el acceso e) Identifique las distintas formas de parametrización del sistema. f) Se lleva controles por escrito de la forma de parametrización del sistema y quien es la persona encargada de este reporte. g) Se Tiene las instrucciones necesarias para realizar la parametrización.			
21	Desarrolle pruebas en los que se intente introducir valores negativos, letras, valores indefinidos, valores de cambio periódico, para verificar si el sistema lo permite			

No.	Procedimiento	Hecho por	Ref.	Observaciones
	entrada de datos			
22	Identifique cual es el origen de datos y la secuencia seguida para el ingreso de datos al sistema considerando que es documental por hacer uso de documentos preimpresos o formularios completados a mano de los cuales se hace uso para alimentar el sistema: a) Que estén elaborados de acuerdo a la secuencia de ingreso al sistema. b) Que estén bien identificados o numerados c) Que estén títulos encabezados descriptivos. d) Con espacio suficiente para correcciones y espacios para firmas de responsables			
23	Evalué el ingreso de datos en la aplicación, determinando que validaciones existen en las pantallas de captura y verifique que cada elemento de estos este configurado correctamente			
24	Evalué los campos numéricos probando que no se puedan ingresar valores negativos donde no corresponda			
25	Verifique que no se realicen cálculos manuales previamente a ser ingresados al sistema, cuando dichos valores puedan operarse automáticamente			
26	Realice comprobaciones de valores numéricos operados dentro de la aplicación.			
27	Evalué que los valores por cálculos automáticos en la aplicación no puedan ser modificados manualmente por los usuarios.			
28	Evalué los campos de tipo moneda, en los cuales existan limites de montos a ingresar respecto a otros valores también almacenados en el sistema.			
29	Revise los campos con datos tipo fecha, donde se facilite su digitación, validando además los rangos de fecha permitidos por estos: a) Verifique la validación de fechas futuras donde amerite hacerse. b) Verifique que no se acepten fechas incongruentes con días, meses o años inválidos, a través de			

No.	Procedimiento	Hecho por	Ref.	Observaciones
	mascaras de entrada bien definidas.			
30	Indague y pruebe campos para los cuales existe un formato predefinido de ingreso de datos: a) Revise las mascaras de entrada para códigos o números que tienen un formato establecido desde el origen de su emisión (Numero de afiliación, NUP, entre otros). b) Pruebe que en campos de formato numérico no se aceptan caracteres diferentes y viceversa.			
31	Verifique que no permita dejar campos vacíos, cuando esos sean de gran importancia para controles o cálculos en esa misma pantalla o en otras de esa aplicación.			
32	Determine el nivel de actualización ó desfase en el ingreso de datos al sistema.			
	Procesamiento de datos			
33	Verifique los procesos que se realizan en el sistema fuera de las pantallas de captura (actualizaciones o carga de datos), a fin de determinar si se le da seguimiento al procedimiento establecido y evalué lo siguiente: **a)** Verifique los cálculos de mayor importancia, con base a los datos con que fue alimentado. **b)** Solicite se nos muestre el código fuente para procesos delicados que no satisfacen nuestra confianza.			
	Salida de información			
34	Evalué la forma en que la información es proporcionada por el sistema.			
35	Determine si la información proporcionada por el sistema es suficiente para el usuario final en base a los requerimientos del sistema.			
36	Verifique que los reportes que se generan estén bien identificados con nombre de programa que lo genera, títulos, fechas,			

No.	Procedimiento	Hecho por	Ref.	Observaciones
	periodo cubierto, número de página, entre otros.			
37	Verifique que los reportes generados y guardados en archivos no pueden ser editados por el usuario.			
38	Verifique que los programas utilizados sean de la misma versión.			
39	Determine si existe algún procedimiento de destrucción o almacenamiento adecuado de los reportes con información restrictiva o confidencial.			
	Pistas de Auditoría			
40	Determine que controles de registro de pistas de auditoría se han implementado en la aplicación			
41	Evalué los registros de auditoría de seguridad identificando usuario, fecha, hora, Terminal y tipo de evento para lo siguiente: a) Intentos fallidos al sistema b) Accesos exitosos al sistema c) Salidas del sistema			
42	Verifique la existencia de registros de eventos para las distintas opciones de mantenimiento de datos en la aplicación, que muestren el usuario, fecha, hora, Terminal, pantalla u opción utilizada, identificación del registro involucrado y campos modificados, para lo siguiente: a) Procesos de edición de registros b) Modificación de registros c) Eliminación de registros			
	Técnicas de auditoría con ayuda de computadora			
43	*Solicite la información al encargado de sistema operativo y mantenimiento o administrador del sistema de las aplicaciones:* *a) Especifique las tablas o archivos de datos* *b) Detalle los campos de los datos* *c) Indique los tipos de formato donde*			

No.	Procedimiento	Hecho por	Ref.	Observaciones
	se efectuara la carga de archivos.			
	Backup			
44	Verifique si existen políticas de Back up en la empresa.			
45	Detalle con que frecuencia se realizan los respaldos, ya se estos; a) Diario b) Semanal c) Quincenal d) Mensual e) Trimestral			
	Lugares de Resguardo			
46	Verifique si existen políticas de resguardo de los back up			
47	Verifique que la información respaldada sea puesta bajo el control de personas idóneas para el caso			
48	Identifique por medio de que elementos es respaldada la información ya sean disquetes, CDS, USB, etc. Y si esta información esta al acceso de cualquier usuario sea directo o indirecto			

3.12.3. Etapa 3: Desarrollo de manuales

PROGRAMA DE AUDITORIA DE SISTEMAS INFORMATICOS EN DESARROLLO

Nombre de la entidad	:	Instituto Salvadoreño del Seguro Social
Fase auditada	:	Desarrollo de SAP
Actividad principal	:	Atención médico/hospitalaria

3.12.3.1. Objetivo general.

Verificar si en los manuales se cumplen de los requerimientos y estos contribuirán a los diferentes usuarios del sistema.

3.12.3.2. Objetivo específicos.

a) Revisar los manuales considerando si cumplen con la ilustración adecuada para cada usuario.

b) Verificar si son de fácil comprensión para los usuarios finales

c) Analizar si están completos y cumplen con los objetivos.

No	Procedimiento	Hecho por	Ref.	Observaciones
1	Revisar el manual de operación del sistema con el objetivo de verificar que éste se desarrolle de acuerdo a lo establecido por el mismo.			

No	Procedimiento	Hecho por	Ref.	Observaciones
2	Examinar que el perfil del personal técnico sea adecuado para que sus actividades las realice de acuerdo a lo planeado.			
3	Verificar si el sistema SAP cuenta con un departamento de supervisión a los módulos asignados a los usuarios.			
4	Verificar si el manual de operación o usuario tiene la estructura del sistema.			
5	Verificar si existen las especificaciones y diseño de entrada de datos (formatos y pantallas de captura).			
6	Verificar si existen las especificaciones y los diseños de salidas de datos(reportes, pantallas de consulta)			
7	Verificar si existen procedimientos o políticas para resolver errores del sistema			
8	Verificar la existencia de los controles de los usuarios al sistema			
9	Revisar si existen políticas de procedimientos en la preparación de las bases de datos.			
10	Verificar si tienen la documentación del sistema por cada modulo.			
11	Verificar si existen documentos de la representación grafica de la estructura del sistema			
12	Revisar las vistas sugeridas por el usuario, los prototipos definidos, y compararlos con las formas y reportes construidos.			
13	Verificar que los usuarios finales asignados cumplan con la idoneidad del puesto para optimizar recursos y tiempo.			
14	Analizar la distribución de responsabilidades de acuerdo a los perfiles de usuarios del sistema.			
15	Examinar que los usuarios utilicen el sistema de acuerdo a las tareas o actividades asignadas a ellos establecidas en los requerimientos.			

3.12.4. Etapa 4 Entrenamiento-Capacitación (Controles administrativos)

PROGRAMA DE AUDITORIA DE SISTEMAS INFORMATICOS EN DESARROLLO

Nombre de la entidad	:	Instituto Salvadoreño del Seguro Social
Fase auditada	:	Desarrollo de SAP
Actividad principal	:	Atención médico/hospitalaria

3.12.4.1. Objetivo general.

Existir una planificación adecuada en la parte de entrenamiento y capacitación en todos los centros médicos/hospitalarios donde se desarrollara la prueba piloto y se implementara el sistema.

3.12.4.2. Objetivo específicos.

a) Verificar Metodología a seguir en la capacitaciones del personal
b) Corroborar que se cumpla lo acordado en los contratos de capacitación
c) Indagar sobre los materiales que se han proporcionado, si cumplen con los objetivos
d) Verificar el proceso de inducción.

No	Procedimiento	Hecho por	Ref.	Observaciones
1	Verificar la metodología a seguir para la enseñanza del sistema de los usuarios finales como los funcionales.			
2	Identificar los tipos de métodos de enseñanza que se aplicaran a los usuarios.			
3	Verificar los tipos de evaluaciones asignadas a los usuarios.			
4	Verificar y medir si los talleres que se impartirán están de acuerdo al material impartido.			
5	Verificar que la institución contratista haya efectuado el entrenamiento a los usuarios funcionales de acuerdo al contrato.			
6	Verificar si se efectuó la inducción necesaria a los usuarios funcionales.			
7	Verificar si a los usuarios funcionales se les impartió las capacitaciones tanto técnicas como funcionales.			
8	Verificar si los usuarios finales tienen conocimiento del nuevo sistema o si están reacios al cambio (plan de contingencia).			
9	Verificar si las herramientas para la enseñanza son las adecuadas, con el objetivo que el usuario final comprenda.			
10	Verificar que el material didáctico que se impartirá a los usuarios finales sea accesible y claro.			
11	Verificar si los encargados de gestión del cambio están cumpliendo con lo planificado, con relación a las programaciones de capacitación.			

CAPITULO IV. CONCLUSIONES Y RECOMENDACIONES

Luego de realizado el estudio de la aplicación de auditoría a un sistema informático en desarrollo se considera como una herramienta para la adecuada toma de decisiones en el área de informática del sector médico/hospitalario, se concluye y recomienda:

4.1 Conclusiones

1. La aplicación de auditoría es importante para la adecuada toma de decisiones, ya que por medio de ella se puede evaluar, verificar, corregir sesgos y la prevención de riesgos al sistema, ya que al implementarlo el usuario final se le facilitara su operatividad.

2. En la mayoría de las jefaturas de informática de las instituciones médico/hospitalario según afirmación de pregunta, gráfico 16, aplican auditoría a los sistemas ya ejecutados, no así a los que se encuentran en desarrollo, porque su costo es muy elevado y la aplicación de ello es muy compleja.

3. Al realizar la investigación se determinó que las jefaturas del área de informática de las instituciones médico/hospitalario, poseen políticas desactualizadas según el cuestionario que se encuesto y hace énfasis en la pregunta 18 y no son del conocimiento del personal, esto ocasionara deficiencias en el desarrollo del sistema, ya que todos deberán estar involucrados para que esta fase sea un éxito.

4. En la actualidad las instituciones médico/hospitalario no consideran el rediseño del sistema en desarrollo ya que la mayoría cree que los requerimientos son completos y también por lo complejo y la capacidad económica para rediseñarlo.

5. No se da importancia necesaria de que el sistema posea los manuales necesario para su buen funcionamiento dicha afirmación se soporta en la información proporcionada en la pregunta, gráfico y cuadro numero 4.

6. El Proceso de parametrización y las interfases poseen controles y políticas según información proporcionado en la pregunta, grafico y cuadro 12.

4.2 Recomendaciones

1. Es fundamental que las instituciones médico/hospitalario apliquen auditoría aun sistema, ya que al aplicarla este permitirá la evaluación y verificación de la información que se desee que genere y sobre todo esta debe ser confiable y oportuna para la adecuada toma de decisiones.
2. En las instituciones que brindan servicios médico/hospitalario, en las áreas de informática deberán aplicar auditoria a un sistema, porque esta fase es muy importante y trascendental ya que es donde se definen los controles, configuraciones y parametrizaciones del sistema que se implementara; y es donde necesita la evaluación de un auditor para que este verifique si se esta aplicando y cumpliendo según los requerimientos solicitados por la institución.

3. Las jefaturas en el área de informática de las instituciones médico/hospitalario deben dar a conocer las políticas internas al personal, ya que esto les permitirá que ellos se desenvuelvan mejor en sus puestos y a la vez conozcan, desarrollen mejor su trabajo con el objetivo de:

a) Conocer y aplicar adecuadamente las políticas internas de la institución
b) Mejor desarrollo y soltura en el puesto de trabajo asignado.
c) Conocer las directrices de las jefaturas para lograr el objetivo en común.

4. Las instituciones deben tener en cuenta al desarrollar un sistema informático, que pueden ocurrir inconvenientes que no estaban previstos, pero que son de mucha importancia en el desarrollo del sistema y a la vez necesarios, útiles para la implementación del sistema y su mejora para los usuarios finales.

5. Es necesario que el sistema cumpla con los requisitos establecidos, que se tengan los manuales de usuario, sistema, y operativos adecuados; ayudando a minimizar problemas al momento de la ejecución de las aplicaciones por el usuario directo; por lo que se necesita una herramienta que en base a los requerimientos operacionales reflejen tanto las expectativas de operación como las de los usuarios, para que el personal de operaciones cuente con manuales de operaciones para todos el sistema y los procesamientos bajo su responsabilidad y los usuarios tenga

un manuales de entrenamiento para todas las aplicaciones son su funcionalidad y una guía para uso del sistema en la práctica diaria.

6. Con el objetivo de personalizar el sistema a los requerimientos y características de la empresa se requiere de un análisis detallado de los mismo y de una buena ejecución de la parametrización en el sistema, esto combinado con una definición de las interfases adecuada, se puede lograr; es por ello que se debe de tomar en cuenta la evaluación de las políticas que se han establecido en estas fases para determinar si son eficientes y considerar reforzarlas.

BIBLIOGRAFÍA

- Alvin A. Arens. Año 1995. Auditoría Un enfoque Integral
- www.delitosinformaticos Propiedad Industrial/auditoría
- *www.deltaasesores.com/Impacto de Tecnologías Informáticas La Informática y su Impacto Social*
- www.gestiopolis.com/ Auditoría de un sistema informático,
- www:m*onografias.com* /trabajos32/auditoría.shtml
- www.monografias.com Auditoría de la Tecnología de Información
- www.monografias.com/A&C Consultaría y Auditoría Empresarial, Colombia
- www.monografias.com Auditoría informática /trabajos05/ aplicación/auditoría
- www.monografias.com/ Auditoría de sistemas y desarrollo / trabajos40 / aplicación/auditoría

Anexos

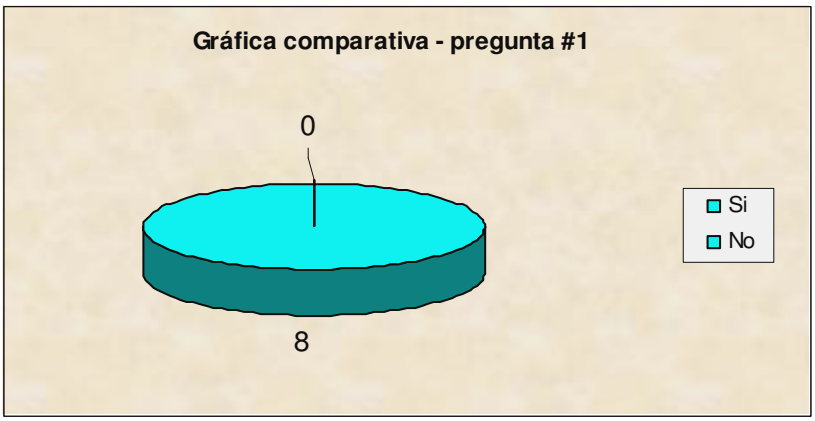
I. Tabulaciones y análisis de encuesta

Pregunta # 1:

¿Cuenta la institución con una estructura organizativa que defina las áreas claves de autoridad y responsabilidad?

Tabulación y grafica No. 1

Alternativas	Dato absoluto
Si	8
No	0
Total...	**8**



Análisis:

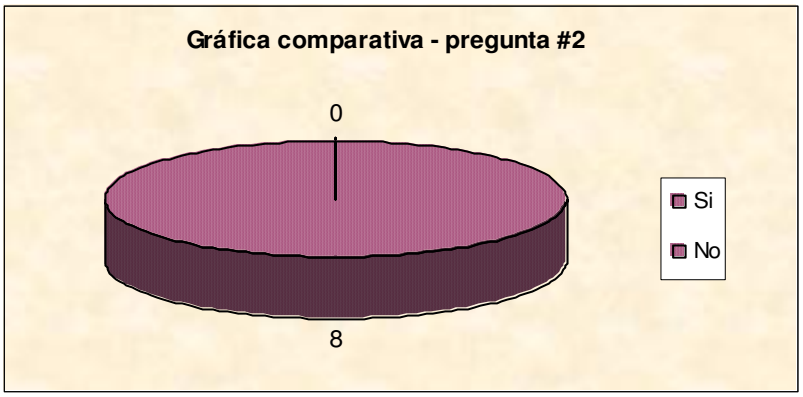
Todas las jefaturas de las unidades de informática entrevistadas manifestaron que su institución cuenta con una estructura organizativa que define las áreas claves de autoridad y responsabilidad para tomar decisiones importantes de acuerdo al área que lo requiera.

Pregunta # 2:

¿Tiene sistemas de información en su centro de atención?

Tabulación y grafica No. 2

Alternativas	Dato absoluto
Si	8
No	0
Total...	**8**



Análisis:

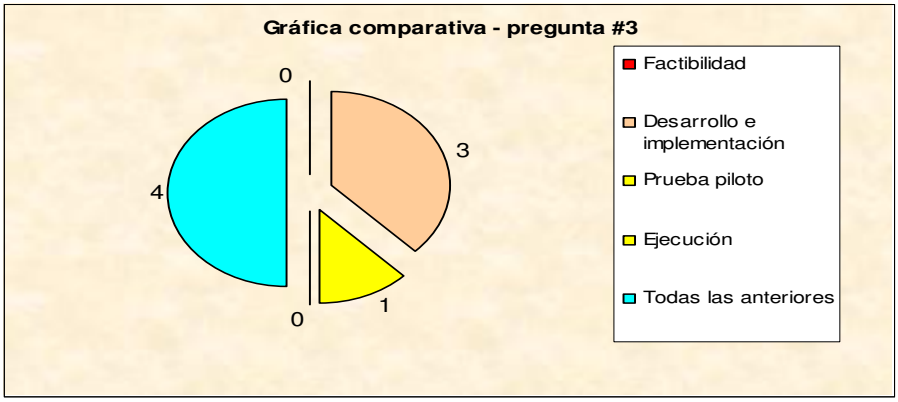
Según la información obtenida de los encuestados todos tienen sistemas de información, con el objetivo de obtener informes ágiles y oportunos.

Pregunta # 3:

Si su respuesta anterior es positiva cuales fases del sistema identifica:

Tabulación y grafica No. 3

Alternativas	Dato absoluto
Factibilidad	0
Desarrollo e implementación	3
Prueba piloto	1
Ejecución	0
Todas las anteriores	4
Total...	**8**



Análisis:

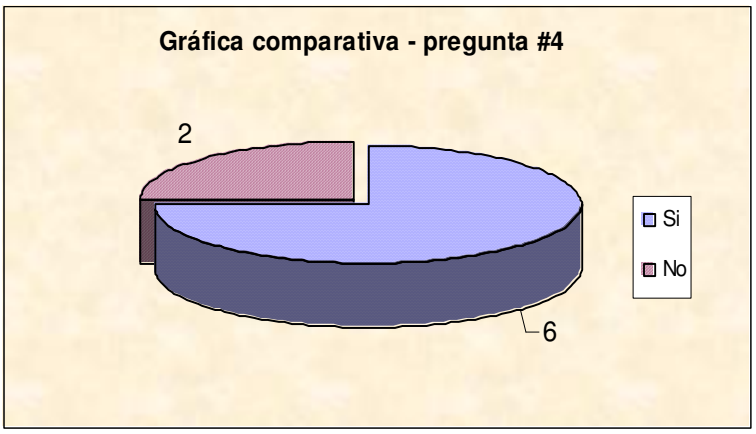
De las jefaturas de la unidad de informática que se encuestaron 3/8 de los entrevistados manifestaron que si conocen la fase de desarrollo e implementación en un sistema informático, un 1/8 manifestó que conoce la fase de prueba piloto y el restante 4/8 conoce la mayoría de las fases.

Pregunta # 4:

¿Aplica auditoría de sistema al SIC (Sistema de Información Computarizado)?

Tabulación y grafica No. 4

Alternativas	Dato absoluto
Si	6
No	2
Total...	**8**



Análisis:

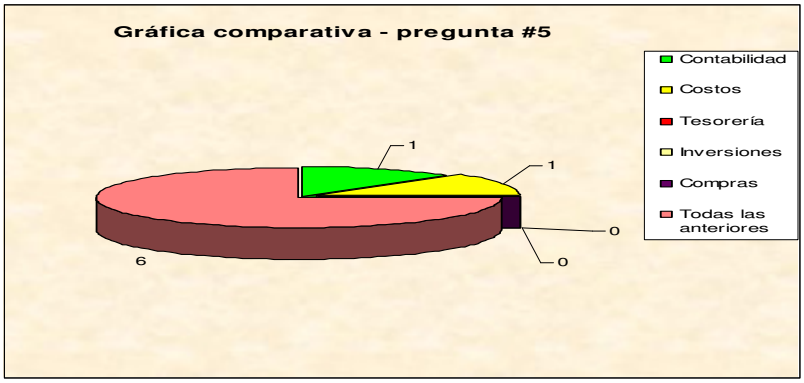
De las jefaturas encuestadas, 6/8 manifestaron que si aplican auditoria de sistemas al sistema informático integrado en desarrollo y de 2/8 no la aplica.

Pregunta # 5:

¿En que áreas la aplica?

Tabulación y grafica No. 5

Alternativas	Dato absoluto
Contabilidad	1
Costos	1
Tesorería	0
Inversiones	0
Compras	0
Todas las anteriores	6
Total...	**8**



Análisis:

Pocos manifestaron que en la área de contabilidad aplican sistemas, también de 1/8 lo aplican en modulo de costos para tomar decisiones y mientras que un 6/8 manifestaron lo aplican en contabilidad, costos, Tesorería, Inversiones y compras.

Pregunta # 6:

¿Considera usted que es importante que exista una planificación adecuada en la fase de desarrollo del sistema?

Tabulación y grafica No. 6

Alternativas	Dato absoluto
Si	8
No	0
Total...	**8**

Análisis:

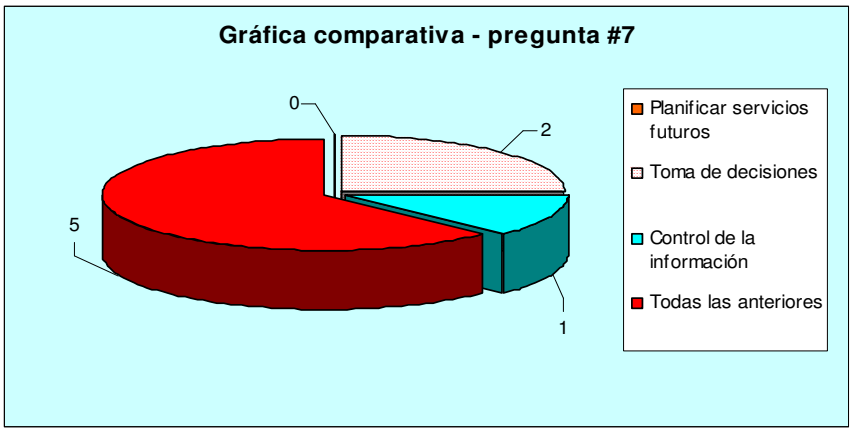
Todas de las jefaturas de informática encuestadas, manifestaron que es importante, que exista una planificación adecuada en la fase de desarrollo de un proyecto; ya que a través de un plan se puede medir los parámetros a seguir.

Pregunta # 7:

¿Para qué utiliza la información que le genera actualmente los SIC?

Tabulación y grafica No. 7

Alternativas	Dato absoluto
Planificar servicios futuros	0
Toma de decisiones	2
Control de la información	1
Todas las anteriores	5
Total...	**8**



Análisis:

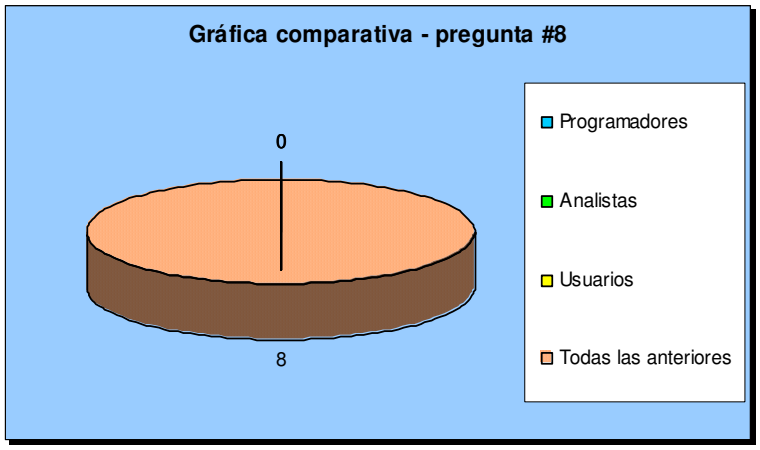
De las jefaturas de la unidad de informática que se encuestaron se pudo obtener que 2/8 consideran que la información que le genera los SIC es para la toma de decisiones, de 1/8 para el control de la información de las áreas relacionadas, 5/8 consideran que es muy importante para las proyecciones a futuro, la toma de decisiones y el control de información.

Pregunta # 8:

¿Quiénes intervienen en el diseño del sistema?

Tabulación y grafica No. 8

Alternativas	Frecuencia absoluta
Programadores	0
Analistas	0
Usuarios	0
Todas las anteriores	8
TOTAL…	**8**



Análisis:

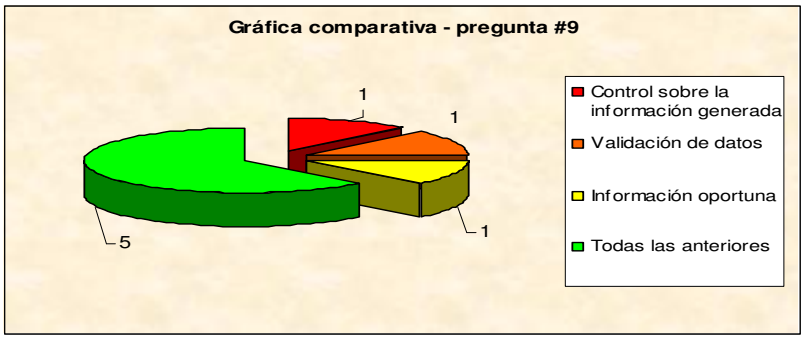
Del total de las jefaturas de la unidad de informática encuestadas, todas manifestaron que los programadores, analistas, usuarios intervienen en el diseño del sistema para que todos estén involucrados con el único fin de que el usuario final comprenda el sistema y sobre todo le sea factible.

Pregunta # 9:

Identifique algunas ventajas al aplicar auditoría a un sistema en desarrollo:

Tabulación y gráfica No. 9

Alternativas	Frecuencia absoluta
Control sobre la información generada	1
Validación de datos	1
Información oportuna	1
Todas las anteriores	5
Total...	**8**



Análisis:

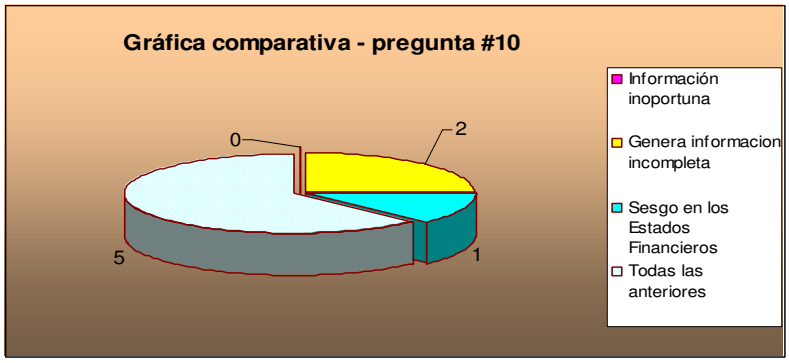
De las jefaturas de la unidad de informática que se encuestaron se pudo obtener que 1/8 consideran como ventaja el control de la información generada por el sistema, de 1/8 la ventaja seria la validación de datos, de 1/8 la información oportuna para la toma de decisiones y de 5/8 manifestaron que las tres ventajas propuestas inciden y son muy importantes para la aplicación de auditoria en un sistema en desarrollo.

Pregunta # 10:

¿Qué deficiencias considera usted en no aplicar auditoría en un sistema en desarrollo?

Tabulación y grafica No. 10

Alternativas	Frecuencia absoluta
Información inoportuna	0
Genera informacion incompleta	2
Sesgo en los Estados Financieros	1
Todas las anteriores	5
Total...	**8**



Análisis:

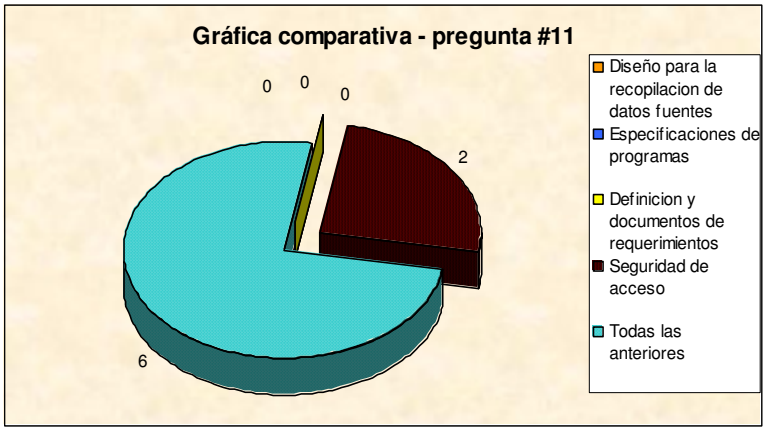
De las jefaturas de la unidad de informática que se encuestaron consideran como deficiencias en no aplicar auditoria a un sistema en desarrollo, de 2/8 consideran que la información que este genera será incompleta, de 1/8 cree que emitirán los estados financieros con sesgos y de 5/8 manifestaron que las tres deficiencias propuestas inciden y son muy importantes para la aplicación de auditoria en un sistema en desarrollo.

Pregunta # 11:

Posee políticas de control en la fase de desarrollo de sistemas

Tabulación y grafica No. 11

Alternativas	Frecuencia absoluta
Diseño para la recopilacion de datos fuentes	0
Especificaciones de programas	0
Definicion y documentos de requerimientos	0
Seguridad de acceso	2
Todas las anteriores	6
Total...	**8**



Análisis:

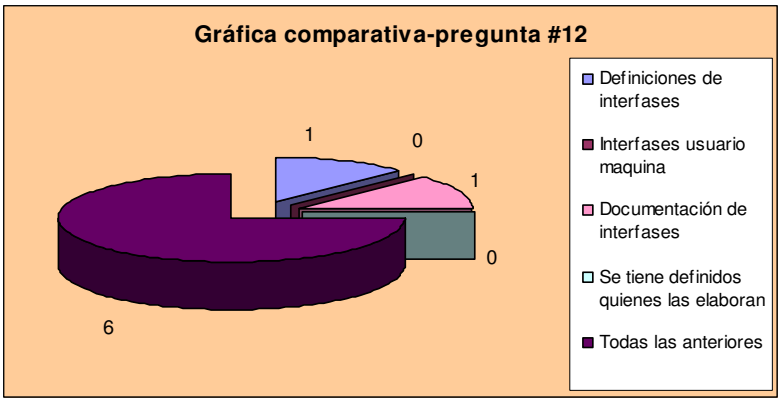
Se obtuvo que 2/8 posee políticas de control en la fase del desarrollo del sistema, en la seguridad de acceso, de 6/8 considera que las cuatro políticas de control propuestas inciden y son muy importantes para la aplicación de auditoria en un sistema en desarrollo.

Pregunta # 12:

Aplican controles en las interfases y parametrizaciones:

Tabulación y grafica No. 12

Alternativas	Frecuencia absoluta
Definiciones de interfases	1
Interfases usuario maquina	0
Documentación de interfases	1
Se tiene definidos quienes las elaboran	0
Todas las anteriores	6
TOTAL...	**8**



Análisis:

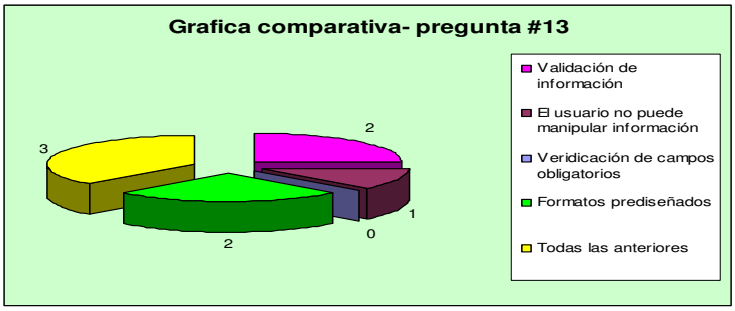
Se pudo obtener que 1/8 aplica controles en las definiciones de interfases y parametrizaciones, 1/8 tiene la documentación de las interfases y 6/8 considera que las cuatro controles de las interfases propuestas inciden y son muy importantes para la aplicación de auditoria en un sistema en desarrollo.

Pregunta # 13:

¿Qué procedimientos de evaluación posee en la fase de entrada de datos?

Tabulación y grafica No. 13

Alternativas	Frecuencia absoluta
Validación de información	2
El usuario no puede manipular información	1
Veridicación de campos obligatorios	0
Formatos prediseñados	2
Todas las anteriores	3
TOTAL...	**8**



Análisis:

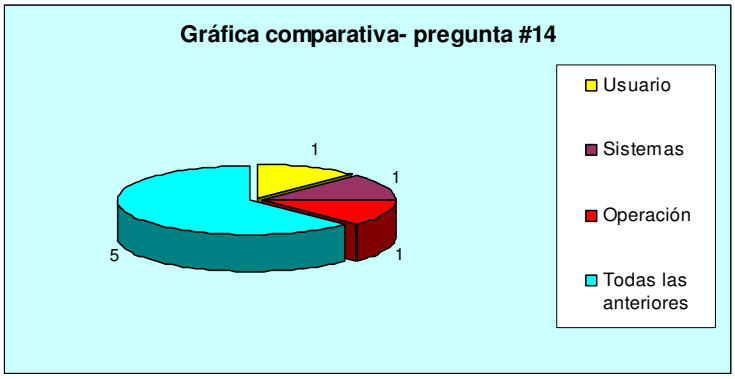
Se obtuvo que 2/8 aplica procedimientos de evaluación en la entrada de datos, tal como la validación de la información, de 1/8 aplica la evaluación cuando el usuario ingrese al sistema, 2/8 se aplica controles en los formatos prediseñados y 3/8 considera que las cuatro evaluaciones en la entrada de datos propuestas inciden y son muy importantes para la aplicación de auditoría en un sistema en desarrollo.

Pregunta # 14:

¿Qué tipo de manuales poseen?

Tabulación y grafica No. 14

Alternativas	Dato absoluto
Usuario	1
Sistemas	1
Operación	1
Todas las anteriores	5
TOTAL...	**8**



Análisis:

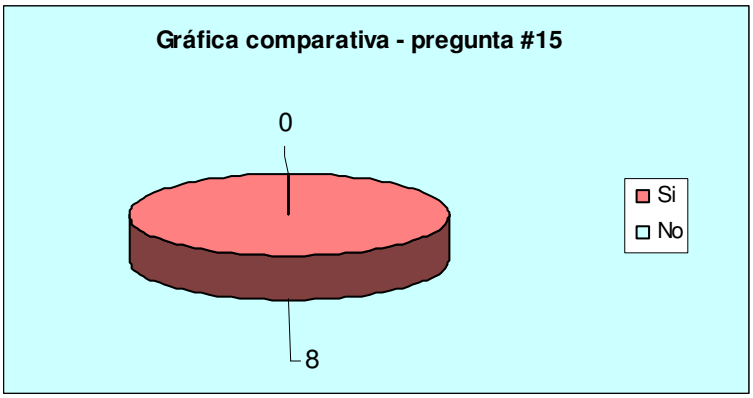
Se obtuvo que 1/8 posee manual de usuario, 1/8 posee manual de sistemas, 1/8 también poseen manual de operación del sistema y 5/8 considera que los tres manuales propuestos inciden y son muy importantes para la aplicación de auditoria en un sistema en desarrollo.

Pregunta # 15:

¿Cree usted que si se implementa auditoría a un sistema en desarrollo, se obtendría información confiable para la toma de decisiones?

Tabulación y grafica No. 15

Alternativas	Dato absoluto
Si	8
No	0
Total...	**8**



Análisis:

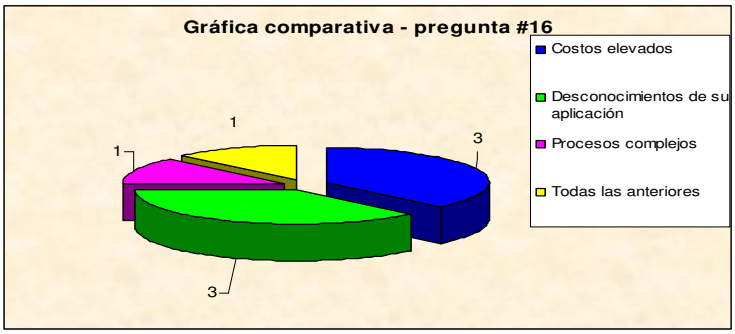
Todas las jefaturas manifestarón que si se aplica auditoría a un sistema en desarrollo se obtendría información confiable para la toma de decisiones.

Pregunta # 16

¿Qué efectos considera que dificultaría la decisión sobre la aplicación de auditoría a un sistema en desarrollo?

Tabulación y Grafica No. 16

Alternativas	Dato absoluto
Costos elevados	3
Desconocimientos de su aplicación	3
Procesos complejos	1
Todas las anteriores	1
Total...	**8**



Análisis:

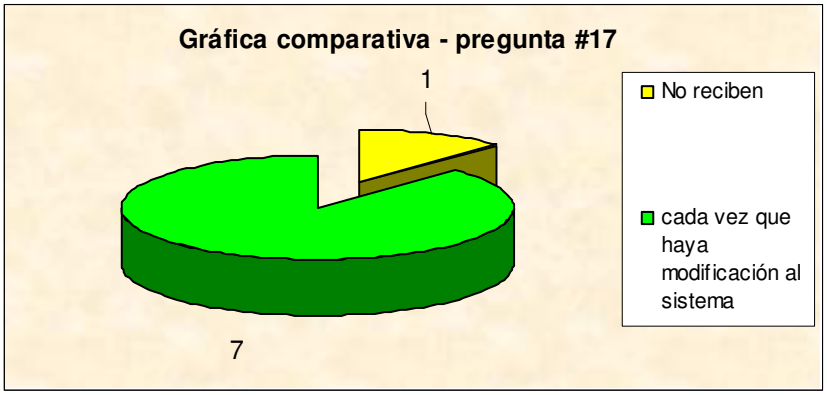
3/8 consideran que la decisión de no aplicar auditoria a un sistema en desarrollo es por los costos elevados que su aplicación implicaría; por otro lado, un porcentaje igual opina que la causa es el desconocimiento que se tiene de la materia, 1/8 piensa que no se aplica por tener procesos muy complejos y finalmente 1/8 manifiesta que la decisión de no aplicarla depende de las tres causas abordadas en líneas precedentes en su conjunto.

Pregunta # 17

¿Con que frecuencia reciben capacitaciones los usuarios del sistema?

Tabulación y Grafica No. 17

Alternativas	Dato absoluto
No reciben	1
cada vez que haya modificación al sistema	7
Total...	**8**



Análisis:

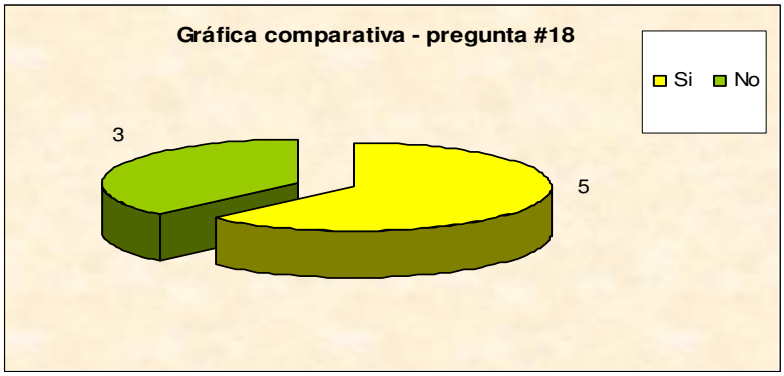
Un 7/8 de los usuarios encuestados manifestaron que reciben capacitación cada vez que los sistemas son modificados; mientras que 1/8 contestaron que no reciben capacitación para el uso de los sistemas con los cuales trabajan, generando con ello la probabilidad de que los datos que se manejan no se encuentren libres de sesgos.

Pregunta # 18

¿Las políticas se encuentran actualizadas y son del conocimiento del personal?

Tabulación y Grafica No. 18

Alternativas	Dato absoluto
Si	5
No	3
Total...	**8**



Análisis:

5/8 de los encuestados manifestaron que las políticas se encuentran actualizadas y les son dadas a conocer de manera periódica a fin de proporcionar una mayor eficiencia y eficacia en la aplicación de las mismas, solo 3/8 contesto que no les son dadas a conocer las políticas para la implementación de los sistemas que poseen en desarrollo.

Pregunta # 19

¿Cree usted que es importante que se tenga una buena administración de riesgo en el área del sistema?

Tabulación y Grafica No. 19

Alternativas	Dato absoluto
Si	8
No	0
TOTAL…	**8**

Análisis:

Todas las jefaturas de las unidades de informática entrevistadas manifestaron que es importante que exista una buena administración del riesgo que les permita manejar la información de manera eficiente y transparente.

Pregunta # 20

¿Existen normas que definen el contenido de los instructivos de captación de datos?

Tabulación y Grafica No. 20

Alternativas	Dato absoluto
Si	8
No	0
TOTAL...	**8**

Análisis:

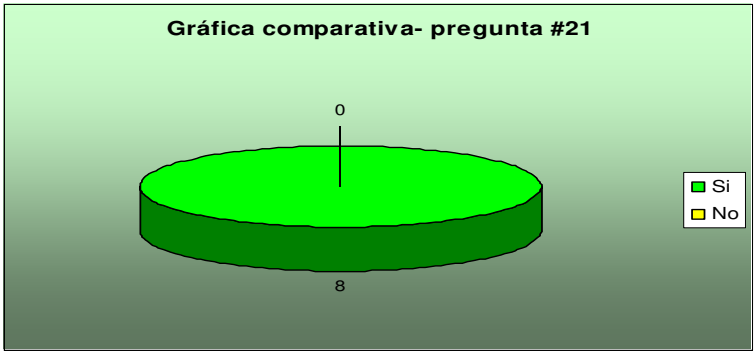
El total 8/8 de los entrevistados contestaron que existen dentro de las unidades de informática normas que definen el contenido de los instructivos de captación de datos, con la finalidad de que estos sean se encuentren libres de sesgos y la información que se genere tenga mayor veracidad.

Pregunta # 21

¿Los controles aplicados en el desarrollo del sistema permitieron que esta fase se realizara de forma eficiente y eficaz?

Tabulación y Grafica No. 21

Alternativas	Dato absoluto
Si	8
No	0
TOTAL...	**8**



Análisis:

Todas las jefaturas encuestadas opinan que la eficiencia y eficacia que se obtiene en el desarrollo de un sistema dependen de los controles que se aplicaron, desde su estudio de factibilidad hasta su implementación.

Pregunta # 22

¿Favorecería un plan sobre procedimientos y técnicas de evaluación del sistema integrado a los usuarios?

Tabulación y Grafica No. 22

Alternativas	Dato absoluto
Si	8
No	0
TOTAL...	**8**

Análisis:

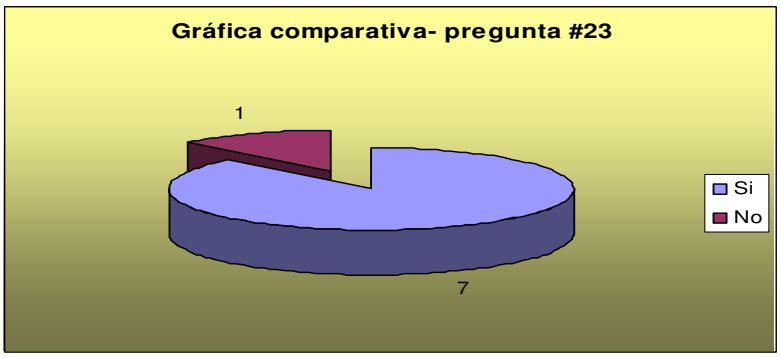
El total de los usuarios encuestados opinan que un plan sobre procedimientos y técnicas de evaluación en un sistema integrado favorecería en gran medida a que su implementación se genere de manera adecuada y oportuna.

Pregunta # 23

¿Se controlan las entradas de información de documentos fuentes?

Tabulación y Grafica No. 23

Alternativas	Dato absoluto
Si	7
No	1
TOTAL	**8**



Análisis:

De la totalidad de jefaturas encuestadas un 7/8 manifestaron que poseen controles para la entrada de información de documentos fuentes a fin de generar información base lo suficientemente verídica para el procesamiento de esta. Mientras que solo 1/8 opino que en sus jefaturas de informática no poseen este tipo de control; por lo tanto, la información considerada para el procesamiento no es leal.

Pregunta # 24

¿Utiliza un manual de control interno de las bases de datos?

Tabulación y Grafica No. 24

Alternativas	Dato absoluto
Si	6
No	2
TOTAL...	**8**

Análisis:

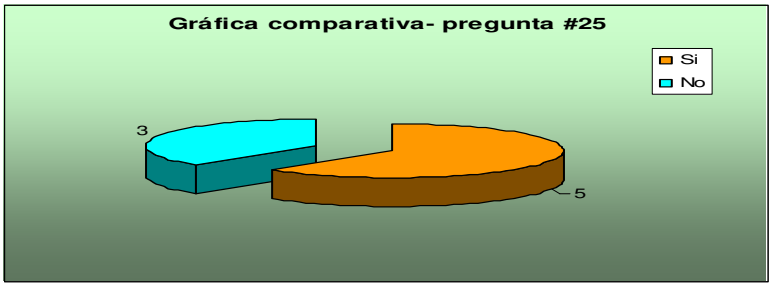
De las jefaturas de unidades de informática encuestadas 6/8 manifestaron que utilizan manual de control interno en la implementación de sus bases de datos, mientras que 2/8 contestaron que no poseen un manual que los oriente sobre su aplicación.

Pregunta # 25

¿Mantiene un registro de anomalías del procesamiento de la información?

Tabulación y Grafica No. 25

Alternativas	Dato absoluto
Si	5
No	3
TOTAL...	**8**



Análisis:

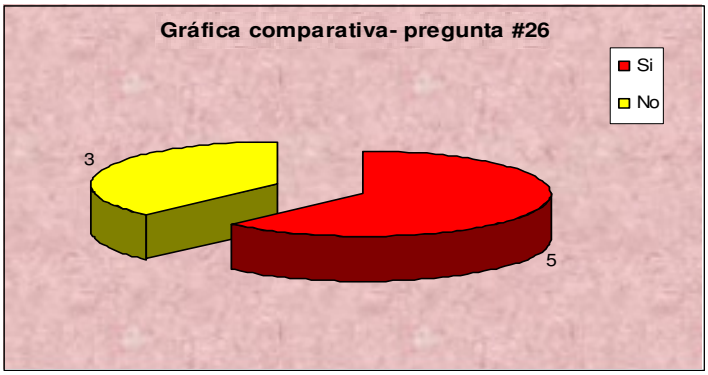
De la totalidad de los encuestados 5/8 de las jefaturas de informática de las instituciones médico/hospitalarias poseen una bitácora del procesamiento de información que les permite conocer en cualquier momento las anomalías que se dan durante su desarrollo y posteriormente poder proceder a subsanar dichas anomalías; mientras que 3/8 no posee un precedente de los errores del sistema, lo cual genera ineficiencia al momento de establecer los errores de este con los técnicos que lo desarrollan.

Pregunta # 26

¿Existen control de fallas de exactitud?

Tabulación y Grafica No. 26

Alternativas	Dato absoluto
Si	5
No	3
TOTAL...	**8**



Análisis:

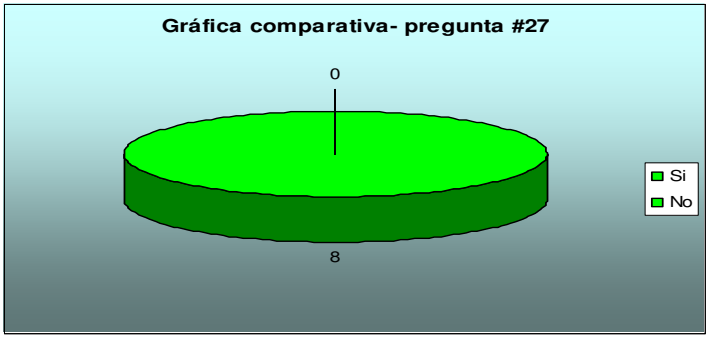
De 5/8 de las jefaturas encuestadas manifestaron que en sus unidades existen controles de fallas de exactitud que hace que la información que el sistema en desarrollo pretende generar sea íntegra y solo 3/8 contestó que no posee este tipo de control en sus unidades de sistema de desarrollo.

Pregunta # 27

¿Los reportes han sido preparados adecuadamente y en forma oportuna según lo esperado?

Tabulación y Grafica No. 27

Alternativas	Dato absoluto
Si	8
No	0
TOTAL...	**8**



Análisis:

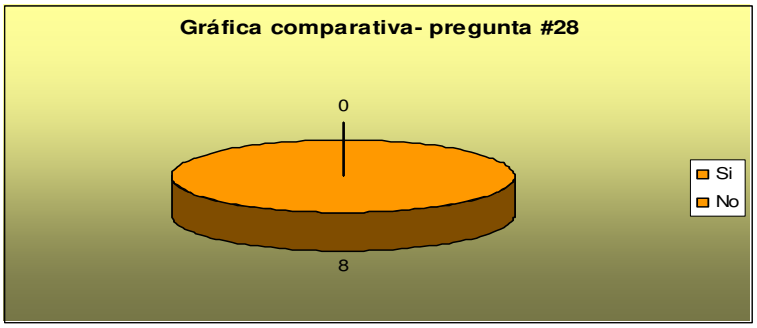
El total de las jefaturas de las unidades de informática entrevistadas manifestaron que los reportes que genera el sistema en desarrollo han sido preparados adecuadamente y en forma oportuna según sus requerimientos y factibilidad.

Pregunta # 28

¿Existe comunicación y coordinación entre usuarios y los desarrolladores del sistema?

Tabulación y Grafica No. 28

Alternativas	Dato absoluto
Si	8
No	0
TOTAL...	**8**



Análisis:

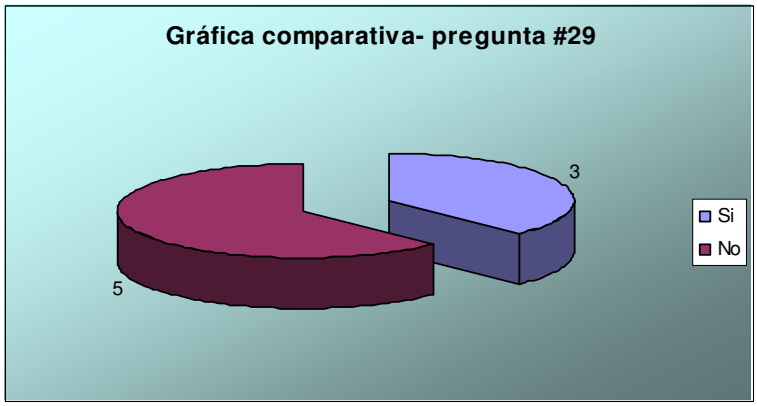
La totalidad de las jefaturas de las unidades de informática entrevistadas manifestaron que se mantiene una buena comunicación y coordinación entre los usuarios y los desarrolladores del sistema, siendo esto necesario para que al momento de implementar los requerimientos establecidos se desarrollen de forma efectiva, ya que son los usuarios los que realizan las pruebas que les permitirán conocer a los desarrolladores si este funciona o no y lo que le hace falta, según su estudio.

Pregunta # 29

¿Se ha considerado el rediseño del sistema?

Tabulación y Grafica No. 29

Alternativas	Dato absoluto
Si	3
No	5
TOTAL...	**8**



Análisis:

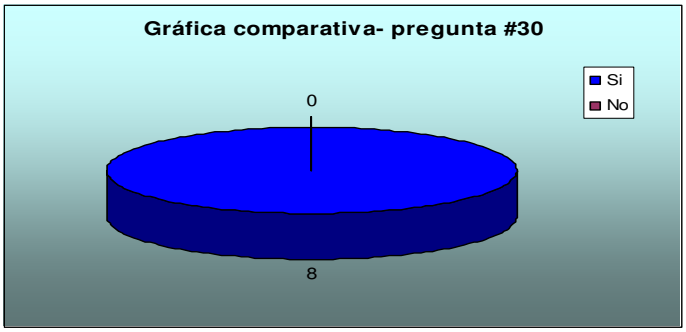
5/8 de los jefes de las unidades de informática de las áreas en estudio opinaron que no han pensado en rediseñar el sistema integrado por no tener por el momento una causa para su cambio, los errores caen dentro de los mínimos; mientras que 3/8 si rediseñarían el sistema integrado si tuvieran la oportunidad para hacerlo.

Pregunta # 30

¿Considera usted que le beneficiaria un trabajo de investigación que trate sobre la aplicación de auditoría a un sistema en desarrollo, enfocado a los servicios médicos/hospitalarios?

Tabulación y Grafica No. 30

Alternativas	Dato absoluto
Si	8
No	0
Total...	**8**

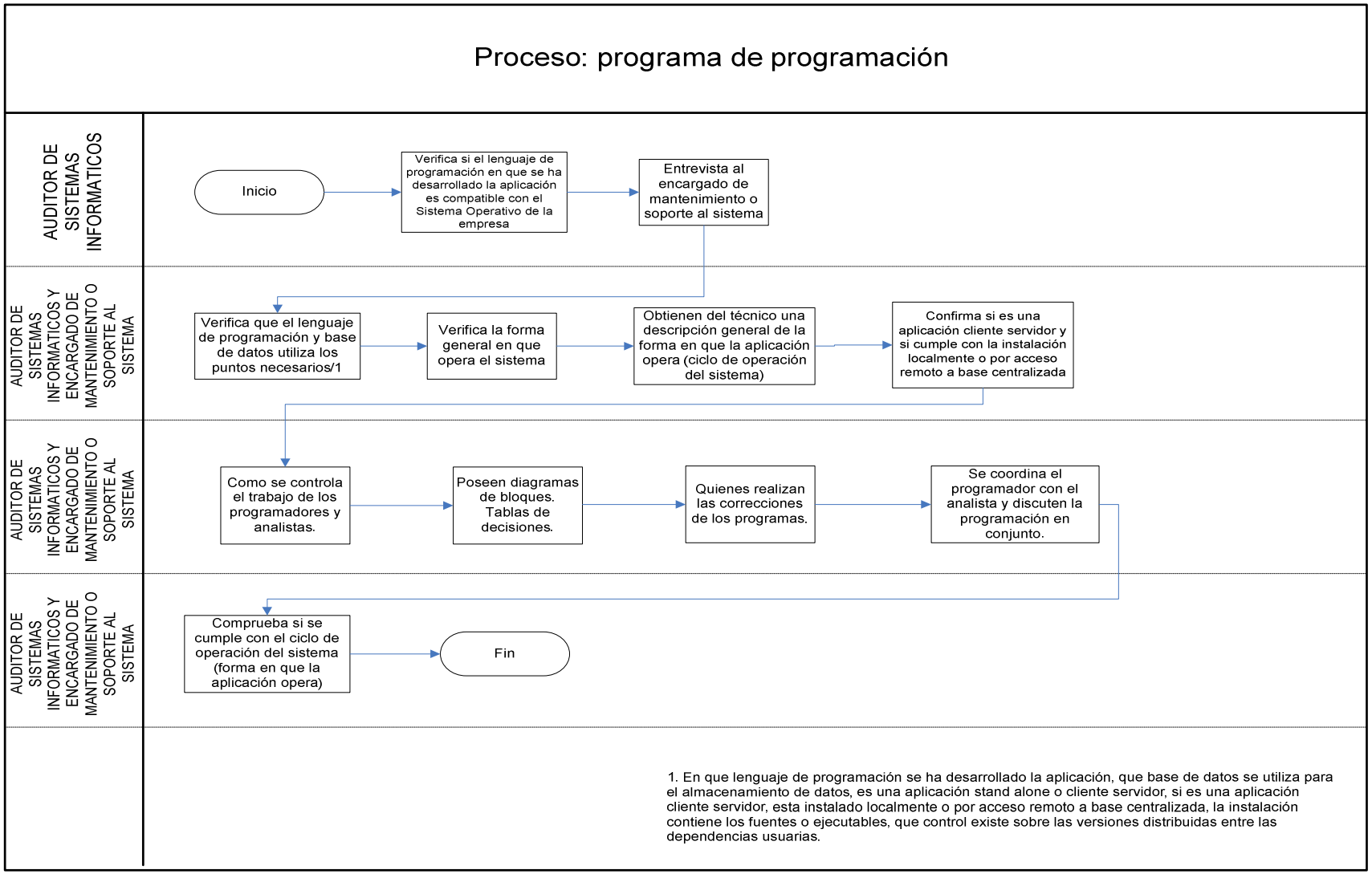


Análisis:

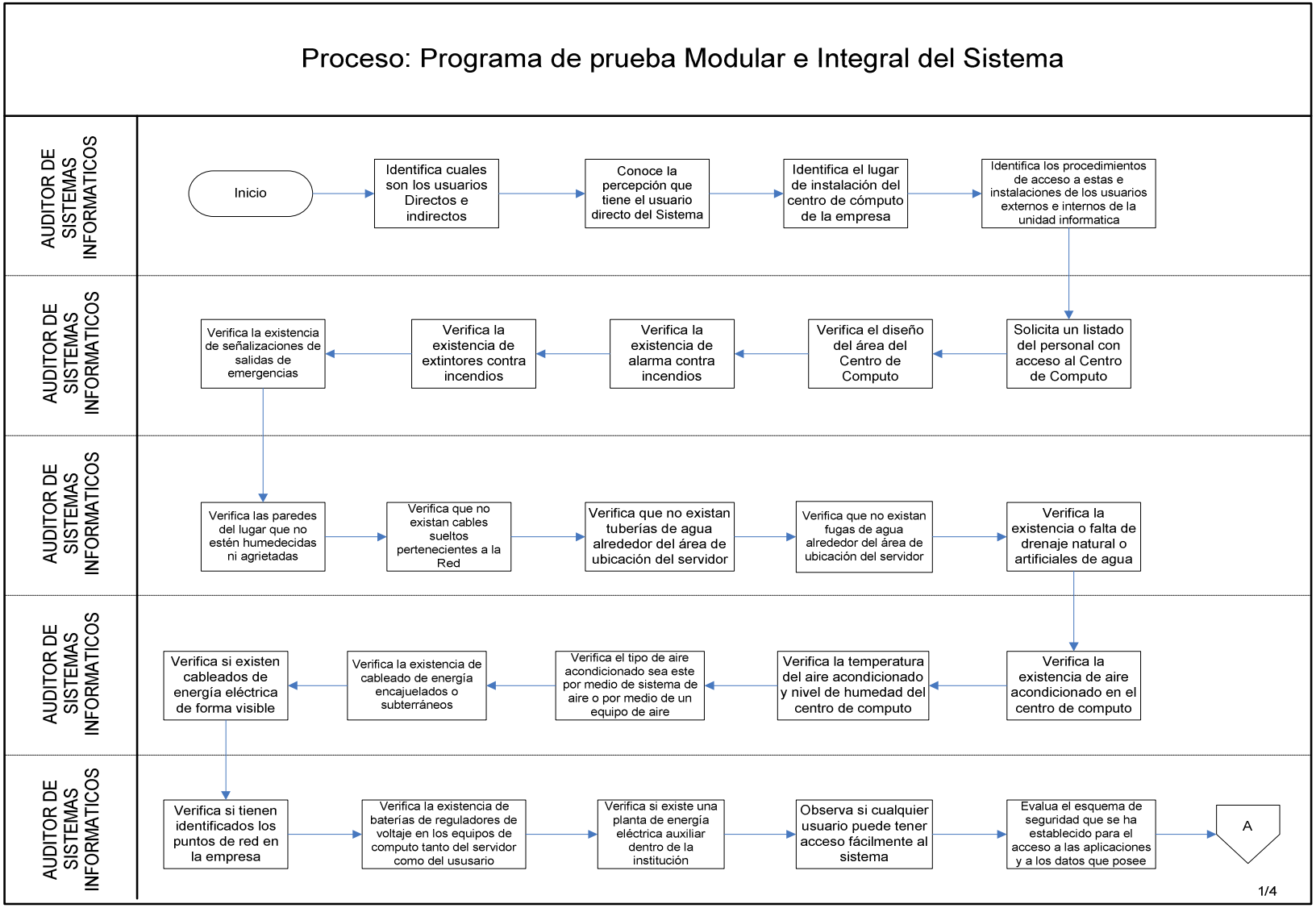
El total encuestado considera que sería de gran beneficio para sus unidades un trabajo de investigación que les muestre como aplicar una auditoria a un sistema en desarrollo. Desde su punto de vista les ayudara a implementar controles adecuados para la generación efectiva y eficiente de la información.

II. Flujogramas de programas

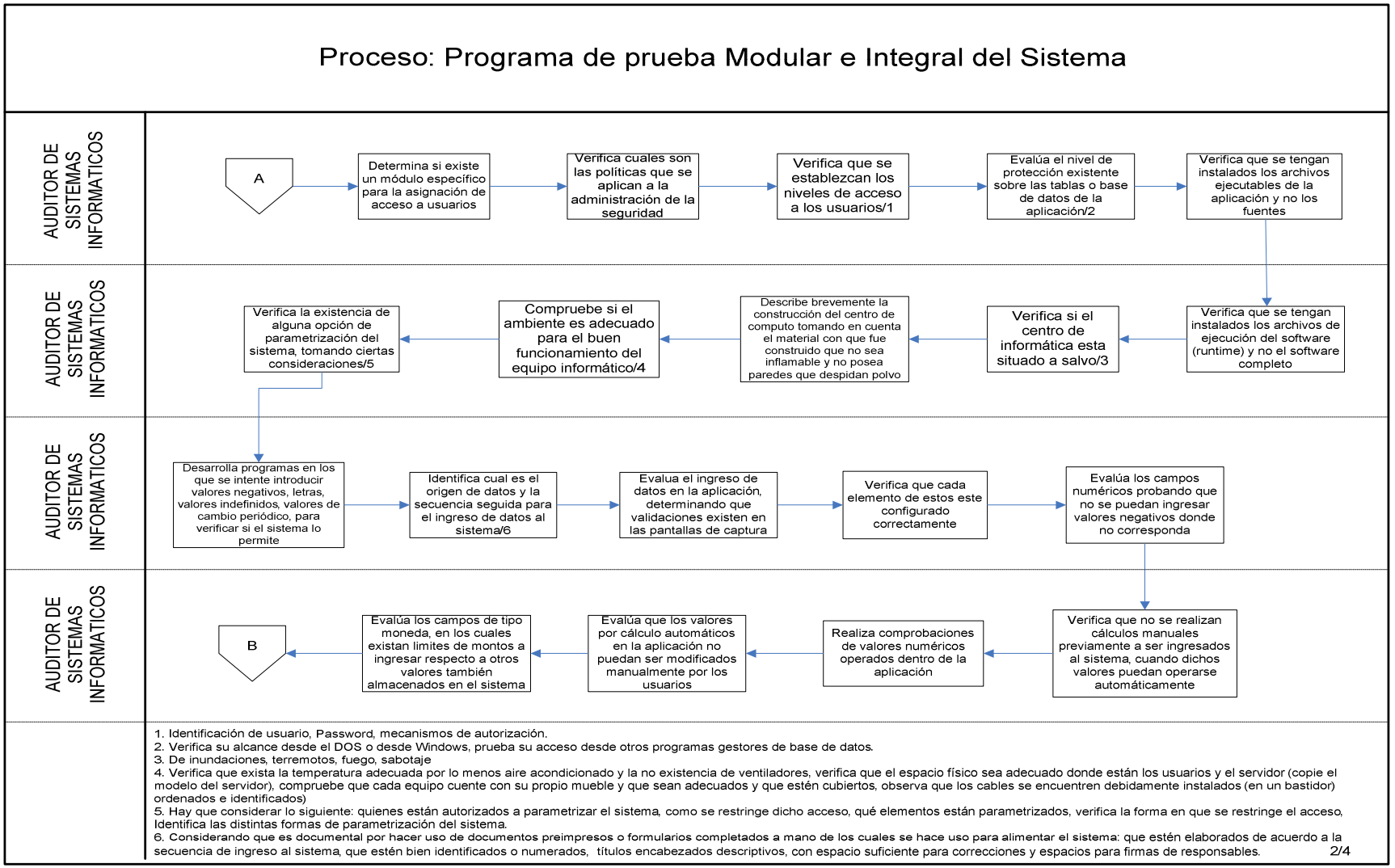
Grafica 1: flujograma de programación



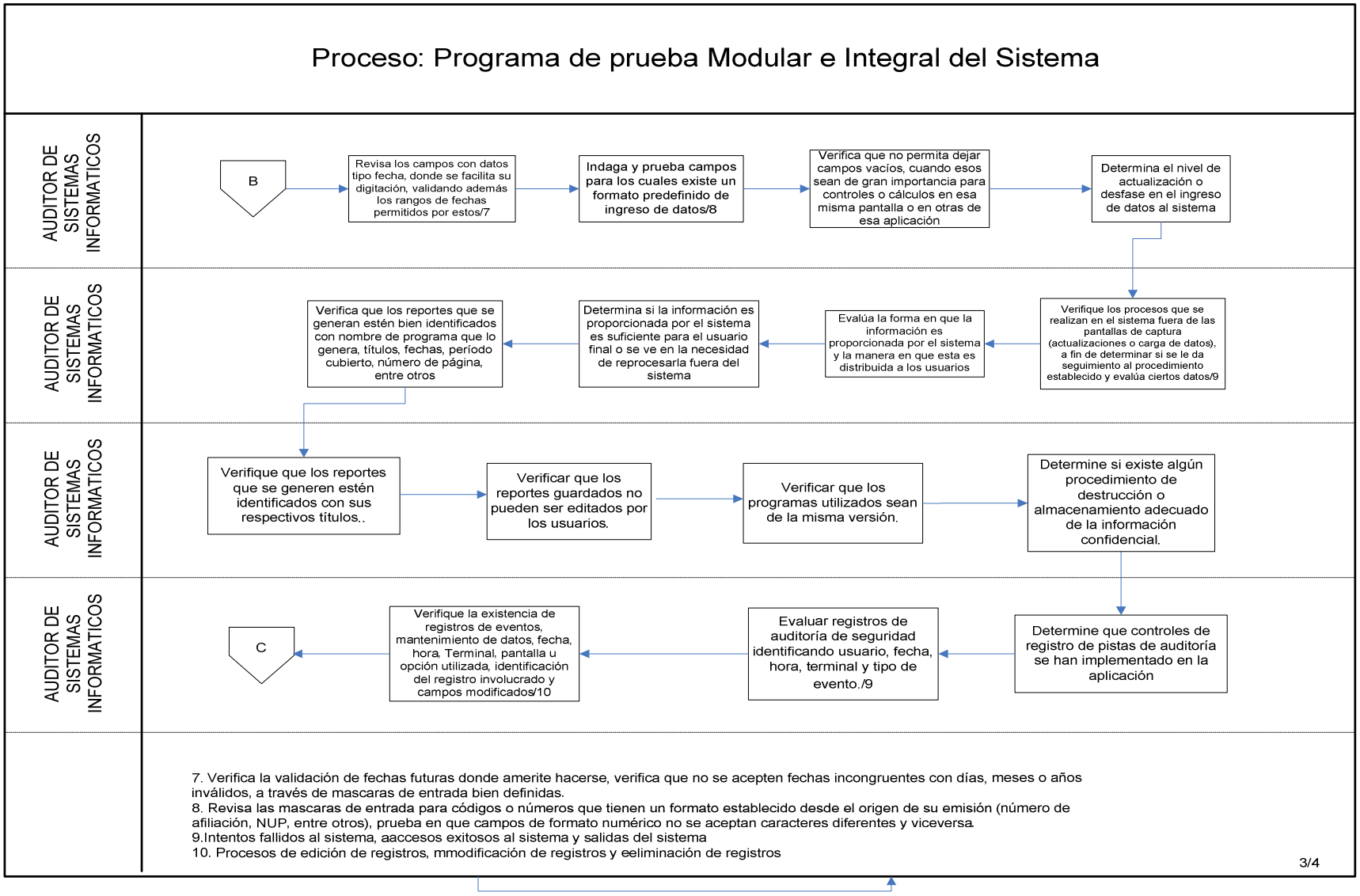
Grafica 2: Flujograma de Programa modular integral del sistema



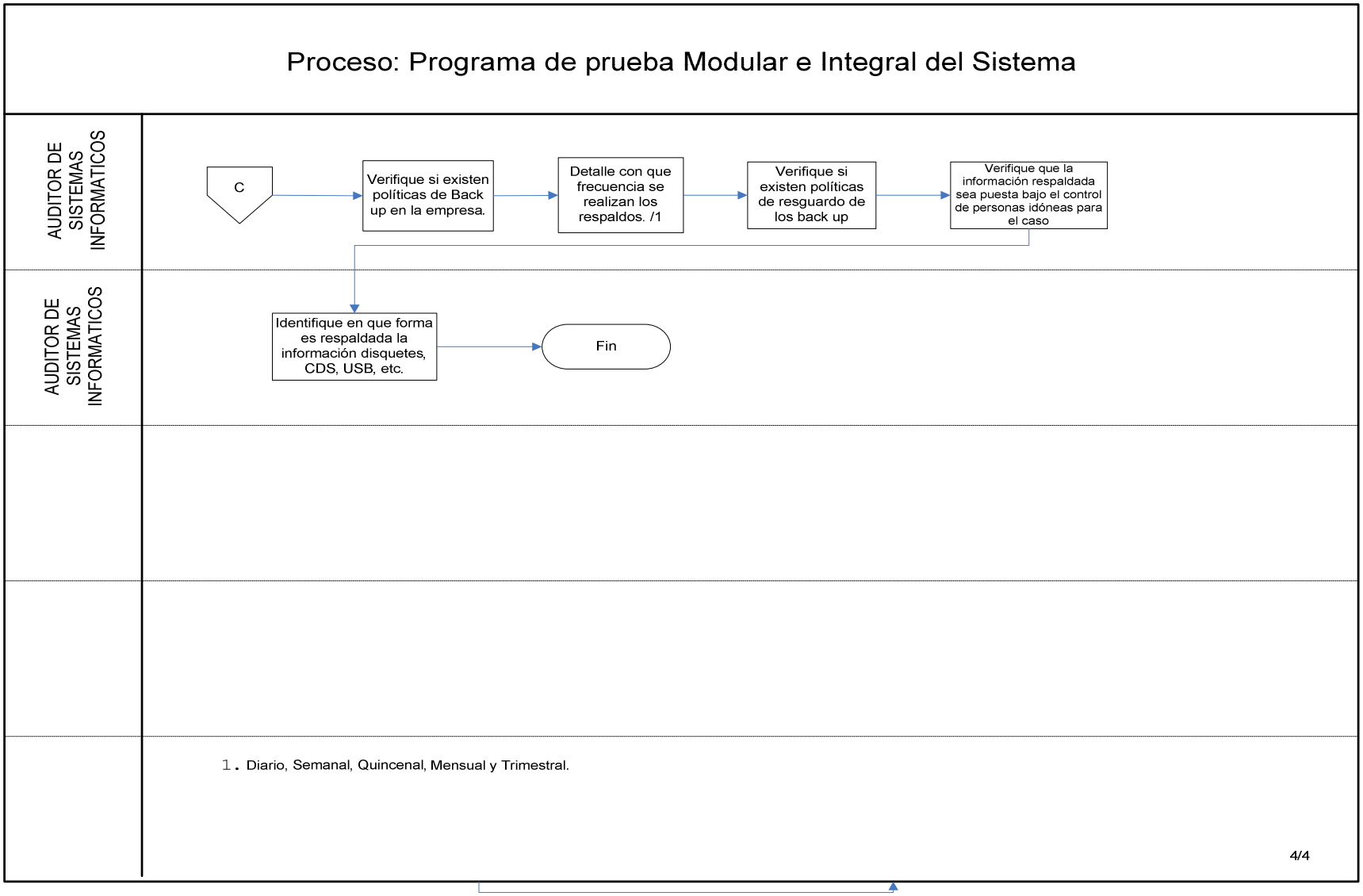
Grafica 2: Flujograma de Programa modular integral del sistema



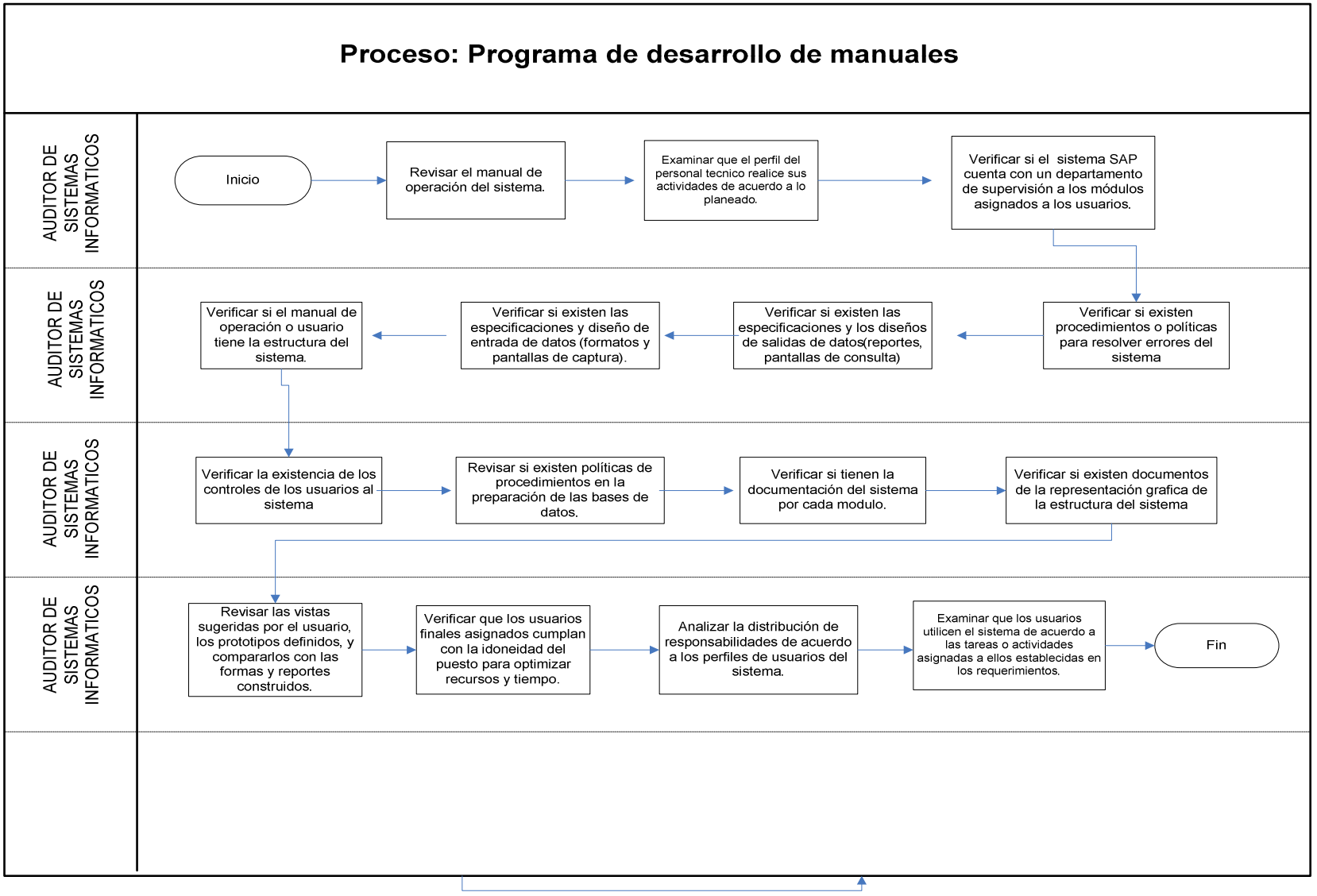
Grafica 2: Flujograma de Programa modular integral del sistema



Grafica 2: Flujograma de Programa modular integral del sistema



Grafica 3: Flujograma de programa de desarrollo de manuales



Grafica 4: Flujograma de Programa entrenamiento-capacitación