

**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

**CARRERA:
CONTABILIDAD Y AUDITORÍA**

**Trabajo de titulación previo a la obtención del título de: INGENIERO EN
CONTABILIDAD Y AUDITORÍA**

**TEMA:
LOS SISTEMAS DE INFORMACIÓN, SU IMPORTANCIA Y EFECTOS EN
LA TOMA DE DECISIONES DE LAS EMPRESAS AUDITORAS DEL
CANTÓN QUITO**

**AUTOR:
JUAN ALEJANDRO CEVALLOS RUBIO**

**DIRECTOR:
RUBÉN DARÍO SÁNCHEZ LÓPEZ**

Quito, marzo del 2015

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO
DE TRABAJO DE TITULACIÓN**

Yo, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaro que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Quito, marzo del 2015

Juan Alejandro Cevallos Rubio
CI. 1715866727

DEDICATORIA

A mis padres por su sacrificio, esfuerzo, dedicación y amor impartidos a lo largo de toda mi vida, son ellos las personas a quién más admiro y respeto, les dedico este trabajo con la firme convicción de superarme y el anhelo de dar lo mejor de mí en todos los aspectos de mi vida tanto personal como profesional.

A mi esposa y familia por estar siempre presente brindándome todo su apoyo incondicional y desinteresado para la consecución de mis objetivos profesionales.

AGRADECIMIENTO

Mi más sincero agradecimiento a las autoridades, docentes, personal administrativo de la Carrera de Contabilidad y Auditoría de la Universidad Politécnica Salesiana y a todas aquellas personas que supieron brindarme su apoyo en este proceso de formación académica.

Agradezco de manera especial al director de la presente tesis Ing. Rubén Darío Sánchez López, por toda la asesoría, dedicación y conocimiento impartido para la consecución y culminación con éxito del presente trabajo de titulación.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO 1	3
LOS SISTEMAS DE INFORMACIÓN Y LA TOMA DE DECISIONES	3
1.1 Los sistemas de información	3
1.2 Definición	3
1.3 Componentes de los sistemas de información	4
1.3.1 Los datos	6
1.3.2 El hardware	7
1.3.3 El software	8
1.3.3.1 Principales tipos de software	8
1.3.3.1.1 Software de sistemas	8
1.3.3.1.2 Software de aplicación	9
1.3.4 La información	10
1.3.4.1 Características de la información	10
1.3.4.2 Cualidades de la Información	12
1.3.5 Las bases de datos	13
1.3.5.1 Sistema de gestión de bases de datos	13
1.3.5.1.1 Objetivos de un sistema de gestión de base de datos	14
1.3.6 Las redes de comunicaciones	15
1.3.6.1 Tipos de redes	15
1.3.7 Las personas (Usuarios)	16
1.4 Clasificación de los sistemas de información	17
1.5 Fases en el desarrollo de sistemas de información	19
1.5.1 Planificación de sistemas	20
1.5.2 Análisis de sistemas de información	22
1.5.3 Diseño de sistemas de información	23
1.5.3.1 Diagramas de contexto	24
1.5.3.1.1 Fase de diseño lógico del sistema	25
1.5.3.1.2 Fase del diseño físico del sistema	25
1.5.4 Implantación y soporte de sistemas	26
1.5.5 Importancia de los sistemas de información	26
1.6 Copias de seguridad (backups).....	26

1.6.1 Planes de contingencia	28
1.6.1.1 Plan de respaldo	29
1.6.1.2 Plan de emergencia	29
1.6.1.3 Plan de recuperación	29
1.6.2 Herramientas de respaldos automáticos	31
1.7 Políticas de seguridad	32
1.7.1 Política de pólizas de seguros de equipo electrónico	33
1.7.2 Niveles de seguridad	36
1.7.2.1 Seguridad Física	36
1.7.2.2 Seguridad lógica	38
1.8 La toma de decisiones	43
1.9 Importancia de la toma de decisiones	43
1.10 Modelos de toma de decisiones	44
1.10.1 Toma de decisiones bajo incertidumbre	44
1.10.2 Toma de decisiones con riesgo	46
1.10.3 Toma de decisiones con certeza	48
1.11 Evaluación y selección de las alternativas para la decisión final	48
CAPÍTULO 2	51
LAS FIRMAS DE AUDITORÍA DEL CANTÓN QUITO	51
2.1 Antecedentes	51
2.2 La auditoría	53
2.3 Tipos y técnicas de auditoría	55
2.3.1 Requerimientos mínimos de competencias de un auditor informático	56
2.3.2 Técnicas de auditoría	56
2.4 Objetivos de la auditoría	59
2.4.1 Objetivos globales del auditor	61
2.5 Las NIFF y las NIA	61
2.6 Firmas de auditoría del cantón Quito	72
CAPÍTULO 3	78
METODOLOGÍA DE INVESTIGACIÓN	78
3.1 Diseño de la investigación	78
3.2 La encuesta	80
3.2.1 Ventajas de la utilización de encuestas	81

3.3 El cuestionario	81
3.3.1 Clases de preguntas	82
3.3.1.1 Por la libertad de elección	82
3.3.1.2 Por la cantidad de respuestas y su relación	83
3.3.1.3 Por los fines de respuesta	85
3.3.1.4 Por la forma de realizarse	86
3.4 Planteamiento de la hipótesis	87
3.5 Planteamiento de las variables	88
3.6 Selección de la muestra	91
3.7 Aplicación de métodos de investigación	95
CAPÍTULO 4.....	98
ANÁLISIS DE LA INFORMACIÓN Y PRESENTACIÓN DE RESULTADOS ...	98
4.1 Análisis de la información	98
4.2 Gráficos de tendencia	119
4.3 Informe de resultados	123
CONCLUSIONES	127
RECOMENDACIONES	130
LISTA DE REFERENCIAS	132

ÍNDICE DE TABLAS

Tabla 1. Principales Sistemas Operativos	9
Tabla 2. Tipos de Redes	15
Tabla 3. Historia de la auditoría	51
Tabla 4. Firmas de auditoría del cantón Quito	74
Tabla 5. Clases de preguntas	82
Tabla 6. Firmas de auditoría del cantón Quito	91
Tabla 7. Medios disponibles utilizados por las firmas	103
Tabla 8. Política para instalar actualizaciones	110
Tabla 9. Distribución de forma porcentual de las decisiones tomadas	113
Tabla 10. Copias de seguridad en medios disponibles	119
Tabla 11. Tipos de medidas preventivas ante un incidente	120
Tabla 12. Tipos de directores que toman las decisiones	121

ÍNDICE DE FIGURAS

Figura 1. Elementos de un sistema de información	5
Figura 2. Clasificación de los sistemas de información en la actualidad	17
Figura 3. Tipos de copias de seguridad	27
Figura 4. Tipos de usuarios en los sistemas de información	39
Figura 5. Firmas de auditoría encuestadas	98
Figura 6. Relación de porcentajes en diagrama pregunta 1	99
Figura 7. Relación de porcentajes en diagrama pregunta 2	100
Figura 8. Porcentajes de usuarios registrados en red	100
Figura 9. Porcentaje de la revisión periódica a usuarios	101
Figura 10. Porcentajes de los medios disponibles al realizar copias de seguridad	102
Figura 11. Porcentajes de firmas que tienen archivos disponibles en red	104
Figura 12. Porcentaje de hardware y software asegurado	105
Figura 13. Firmas que utilizan manuales para uso de los equipos	106
Figura 14. Porcentajes de firmas que realizan pruebas de control	109
Figura 15. Grado de confiabilidad del sistema contable	111
Figura 16. Medidas preventivas tomadas ante un incidente en la organización	112
Figura 17. Directores de la organización que toman decisiones financieras	113
Figura 18. Cambios en el sistema de información	114
Figura 19. Firmas que tienen convenios con compañías de seguridad	116
Figura 20. Firmas de auditoría con sistema amigable	118
Figura 21. Gráfico de tendencia global de las preguntas cuantificables	119
Figura 22. Tipos de copias de seguridad	120
Figura 23. Alternativas de solución en caso de siniestro	121
Figura 24. Toma de decisiones por parte de los directivos de la organización	122

RESUMEN

La información como un recurso necesario e imprescindible ha permitido a través de un proceso moderno y global la interacción de datos en grandes volúmenes, crecen a medida que pasa el tiempo son capaces de ser almacenados en medios cada vez más complejos y reducidos, de esta forma es inevitable la creación de sistemas de información que administren y gestionen todo este contenido de una manera eficiente, un recurso cada vez más digital y que tiene la capacidad informar permite la integración de datos para su interpretación y análisis posterior.

Por lo tanto a partir de esta temática nace la necesidad de desarrollar una tesis que permita identificar, evaluar y analizar los sistemas de información que utilizan las firmas auditoras del cantón Quito con el fin de emitir un informe de resultados que muestre las divergencias de la utilización y los riesgos de estas plataformas con el fin emitir un conglomerado de conclusiones y recomendaciones a los usuarios y que favorezcan el mejoramiento de la utilización de estos componentes que cada vez son más necesarios para desarrollo empresarial.

ABSTRACT

Information as a necessary and indispensable resource has allowed through a modern and comprehensive data interaction process large volumes grow as time passes are capable of being stored in increasingly complex ways and small, in this way inevitably creating information systems that administer and manage all this content in an efficient manner, an increasingly digital resource that has the ability to report data integration allows for interpretation and analysis.

So from this issue arises the need to develop a thesis to identify, evaluate and analyze the information systems used by audit firms canton Quito to issue an earnings report that shows the differences in the use and risks of these platforms to issue a conglomerate of conclusions and recommendations to users and to promote the improvement of the utilization of these components are increasingly needed for business development.

INTRODUCCIÓN

En el presente trabajo de titulación se desarrolla el tema LOS SISTEMAS DE INFORMACIÓN SU IMPORTANCIA Y EFECTO EN LA TOMA DECISIONES DE LAS EMPRESAS AUDITORAS DEL CANTÓN QUITO, por tal razón esta temática representa el grado de necesidad de las firmas de auditoría para gestionar, respaldar, evaluar, administrar y controlar la información de tal forma que esté disponible para sus usuarios de una manera confiable y oportuna, de ahí la oportunidad para los analistas, programadores y diseñadores de sistemas la creación de plataformas tecnológicas acordes a los requerimientos actuales de seguridad, control, prevención, monitoreo, análisis y resultados de los datos para estén presentados con dinamismo y confiabilidad para su posterior toma de decisiones.

En este trabajo se presentan cuatro capítulos, el primer capítulo muestra, a través de la investigación bibliográfica, los sistemas de información a analizar cual es importancia, como sirven de apoyo a las operaciones de la empresa y como la información obtenida a través de un conjunto de elementos, permiten la interacción de procesos en su conjunto para tomar decisiones con el fin de mejorar la eficiencia y competitividad de la organización.

El segundo capítulo nos permitirá identificar la auditoría, sus inicios, que inconvenientes tenía su preparación, su evolución y como surgieron las diferentes soluciones a los problemas, analizaremos las NIIF y las NIA su importancia en el desarrollo de la auditoría y por último se describirá las firmas auditoría del cantón Quito.

El tercer capítulo muestra nuestro modelo de investigación de tipo descriptivo en el que el objetivo principal es medir, evaluar y recolectar datos sobre diversos aspectos del problema de investigación por último para este proceso se hará uso de la encuesta la misma que identificada la población, será cuantificada y de ésta se extraerá la muestra más representativa para su posterior análisis.

El cuarto capítulo muestra el análisis de la información obtenida y el informe de resultados correspondiente, el mismo que incluirá todos aquellos aspectos más relevantes del proceso de investigación.

Por último se expresan las conclusiones y recomendaciones con la finalidad de dar a conocer la información con resultados cuantificados e inherentes a la investigación.

CAPÍTULO 1

LOS SISTEMAS DE INFORMACIÓN Y LA TOMA DE DECISIONES

1.1 Los sistemas de información

En el presente capítulo vamos a dar a conocer los sistemas de información, su definición teórica, cuales son los componentes que la conforman, su clasificación, de qué manera se componen sus fases para el desarrollo de un sistema, porque son importantes y como pueden influir en las decisiones que deben tomar con relación a los datos obtenidos y como esta información se presenta a favor de las necesidades de la organización.

A continuación se define el concepto de sistema: como un conjunto de elementos organizados e interrelacionados entre sí para lograr un objetivo, existen dos tipos de sistemas, un sistema físico que puede ser un ordenador, un televisor, un ser humano pero también puede ser abstracto o conceptual como el software de un ordenador o un método de toma decisiones, de esta forma todos los sistemas contienen subsistemas o elementos que conforman un todo que permiten el ingreso, procesamiento y salida de información hacia el usuario que manipula estos componentes.

1.2 Definición

Un sistema de información se lo define así:

Un sistema de información se lo puede definir desde un punto de vista técnico como un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización. Además, los sistemas de información también pueden ayudar a los gerentes y los trabajadores a analizar los problemas, visualizar asuntos complejos y crear nuevos productos. (Laudon, 2008).

Partiendo de otra perspectiva se definen a los sistemas de información:

El sistema de información empresarial es diseñado e implantado en la organización no solo para gestionar la información y el conocimiento sino también como medio para mejorar los procesos empresariales y en última instancia para crear valor. Un sistema de información, por tanto, será tanto más eficiente y mejor cuanto es más capaz sea de mejorar los procesos de negocios y los de toma de decisiones en la empresa conduciendo a una mayor rentabilidad o a unos menores costes. Por esta razón el sistema de información que no proporcione un conocimiento o información de salida de mayor valor, en términos de utilidad, que el coste de producirlos u obtenerlos no debe ser mantenido en la empresa. (De Pablos, Lopez, & Santiago Martín-Romo, 2006. pág. 46).

Al unir las dos definiciones se puede afirmar que los sistemas de información, son un conjunto de componentes que se relacionan entre sí para gestionar los datos dándoles un valor para que estos sean más eficientes, de tal forma que sirva para mejorar los procesos, analizar los problemas y tomar decisiones que conduzcan a una mayor productividad y rentabilidad a la organización.

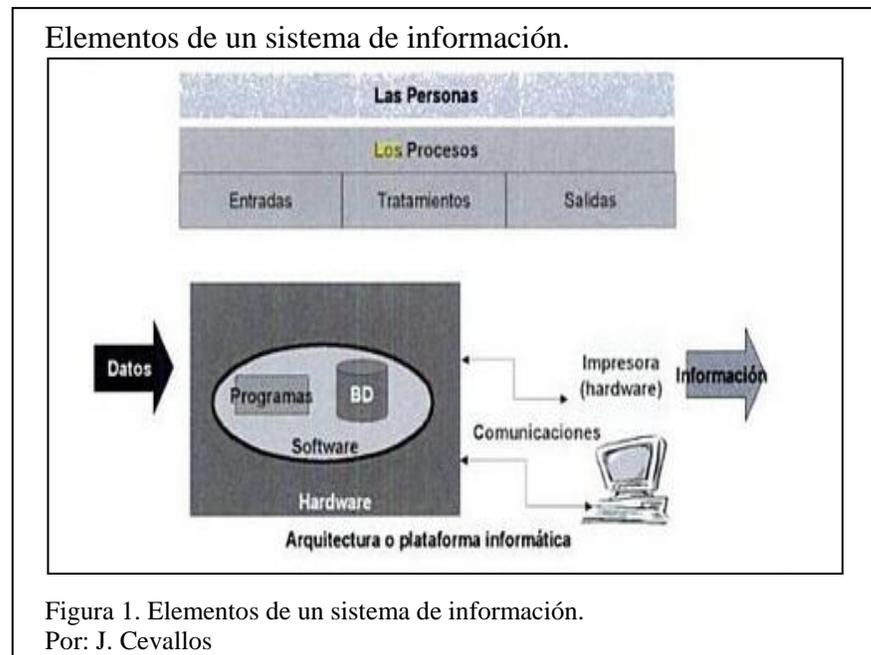
1.3 Componentes de los sistemas de información

Los componentes de un sistema de información son todos los elementos que trabajan en conjunto para lograr el objetivo deseado que es la toma de decisiones, según (Giner de la Fuente, 2004.pág.47) los siguientes elementos forman parte de un sistema de información:

- a) Los datos
- b) La información
- c) El hardware
- d) El software
- e) Las bases de datos

- f) Las redes de comunicaciones
- g) Las personas (Usuarios)

Para ilustrar de mejor manera los elementos a continuación se muestra una gráfica en la que se muestra la relación de los elementos:



En la gráfica podemos observar el proceso de entrada de información que son los datos que ingresan para poder analizarlos, después interviene la fase del tratamiento en el que interviene el software del sistema informático con la ayuda del hardware para tratar los datos obtenidos al inicio, cabe indicar que en este proceso se unen las redes de comunicaciones, las bases de datos por tanto están integradas y nos devuelven la información de salida, ésta se obtiene de manera digital en la computadora en el sistema informático lo que nos permite verificar toda la información obtenida, tomar medidas correctivas en el caso de que el sistema lo permita y luego conforme con los resultados se obtiene información de manera física por ejemplo en las impresiones a través del hardware la información obtenida se presenta como resultado de toda la operación.

1.3.1 Los datos

Son elementos discretos sin valor, es decir el valor lo aporta la capacidad de convertir los datos mediante la debida relación y tratamiento de estos en información, en ocasiones las organizaciones dedican esfuerzos importantes a modelar la información de gestión, a trabajar sobre una estructura relacional de indicadores y sus medidas que les permitan conocer el comportamiento de su negocio o el de alguna área relevante y se encuentre que no tienen los datos necesarios, ahora la pregunta sería ¿Dónde están estos datos y cómo son estos?, pues para responder esta pregunta se necesita conocer las características de los datos, todo dato se distingue por su forma (cómo tenemos el dato), por su contenido (qué tipo de dato), y por su procedencia u origen (de dónde viene). (Giner de la Fuente, 2004, pág.48).

Entonces el dato es un elemento que no ha sido transformado sino hasta su uso y de forma tal que, sirve al momento que en su conjunto permite obtener información, la misma que debe adaptarse y ser de primordial importancia para la organización en cuanto a la satisfacción de sus necesidades de obtención de respuestas a sus posibles problemas.

En cuanto a la forma es posible almacenar los datos en forma estructurada y no estructurada la primera es en relación a la longitud del campo y clase de carácter (caracteres, conjunto de signos diferenciados incluidos espacios) que contiene el dato esta de forma predeterminada y el formato no estructurado deja libre la longitud de campos y clase de caracteres que debe contener puede ser una foto un informe. Con respecto al contenido es posible almacenar datos: solo numéricos, solo texto, mezcla de texto y números (alfanuméricos), imágenes, sonidos y videos. En cuanto a la fuente de datos por su procedencia u origen, conviene dos grandes ámbitos, estos son el ámbito externo en el que la empresa u organización tiene un amplio

universo macro económico el que está representado por el entorno económico, político social y tecnológico la recopilación de este entorno permite tener información y por tanto el conocimiento del que se desprende las conductas y tendencias en todos los órdenes que la pueden afectar. Por último el ámbito interno este se deriva de un contacto personal directo (reuniones, una conversación, por teléfono, el mail), a lo largo del ejercicio de la actividad profesional es en este momento donde se efectúan frecuentes intercambios personales en los que se dan intercambios de información que proporcionan el conocimiento. (Giner de la Fuente, 2004, pág. 57).

En primera instancia se identifica el dato por su longitud es decir cuál es el tamaño del mismo, luego identificarlo por su contenido es ahí entonces donde se vuelve relevante de esta forma lo puede clasificar de acuerdo al tipo y a su vez estos permiten identificar cada uno de sus elementos para poder analizarlos por separado.

1.3.2 El Hardware

Constituye uno de los elementos más importantes del sistema, este elemento será la infraestructura sobre la que se apoye el sistema informático y gran parte del sistema de información, contiene un conjunto de componentes de naturaleza física y por tanto material para atender las actividades de recogida, procesamiento y comunicación del sistema, para analizar de manera profunda al hardware de computadora cuando queramos hacer referencia a los elementos físicos que constituyen al ordenador son: unidad central de procesamiento y los dispositivos periféricos así como otros medios físicos gracias a los cuales se vinculan esos dispositivos (tarjetas, buses cables, etc.), pero también nos podemos referir al hardware de comunicaciones cuando hablemos de los elementos físicos vinculados a una red de comunicaciones cuya labor fundamental será la de transferir datos e información de un lugar físico a otro, similares términos se pueden

hacer referencia al software de computadora y comunicaciones. (De Pablos, Lopez Hermoso, Martin Romo, & Sonia, 2004, pág. 55)

El hardware en sí es elemento físico con el que podemos interactuar de forma directa y que permite a través del uso del software interpretar los resultados de la información en forma digital, a través de la pantalla, o en medios de almacenamiento magnéticos y también de forma física en la impresión de los documentos como un informe o una imagen.

1.3.3 El software. Consiste en las instrucciones detalladas que controlan el funcionamiento de un sistema computacional, según (Amaya A. J., 2009, pág. 31) nos habla de las funciones del software y estas son:

- a) Administrar los recursos computacionales del hardware.
- b) Proporcionar las herramientas para aprovechar dichos recursos.
- c) Actuar como intermediario entre las organizaciones y la información almacenada.

1.3.3.1 Principales tipos de software. Existen dos tipos principales de software y cada uno tiene funciones diferentes según (Amaya A. J., 2009, pág. 32) y se los detalla así:

- a) Software de sistemas
- b) Software de aplicación.

1.3.3.1.1 Software de Sistemas. Es un conjunto de programas generalizados que administran los recursos de la computadora, como el procesador central, los enlaces de comunicación y los dispositivos periféricos, los programadores que escriben software de sistemas se les denomina programadores de sistemas, al software de sistemas que administra y controla las actividades de la computadora también se le denomina como sistema operativo.

Funciones del sistema operativo. El sistema operativo es aquel que decide que recursos de la computadora se usarán, que programas se ejecutarán y el orden en que se efectuarán las actividades, las tres funciones principales de un sistema operativo son:

- a) Reparte y asigna los recursos del sistema.
- b) Programa el uso de los recursos de computación y programa la ejecución de los trabajos de computación.
- c) Monitorea las actividades del sistema de computación.

A continuación se muestra un cuadro con los principales sistemas operativos cual era el fabricante y como se ejecutaba como lo describe (Amaya A. J., 2009) en su libro:

Tabla 1.
Principales Sistemas Operativos

PRINCIPALES SISTEMAS OPERATIVOS		
Nombre del S.O.	Fabricante	Se ejecuta en
Windows 98, 2000, ME, XP	Microsoft	Sistema operativo de 32 bits con interfase gráfica con el usuario. Tiene capacidades multitareas y de trabajo con redes potentes y se puede integrar con los recursos de información de la Web.
Windows NT (Windows 2000)	Microsoft	Sistema operativo de 32 bits para PC, estaciones de trabajo y servidores de red, no limitado a microprocesadores Intel. Apoya multitareas, multiprocesamiento y trabajo intensivo con redes.
Windows 2000 Server	Microsoft	Ultima Versión de Windows que lo convierte en un sistema operativo de redes.
OS/2	IBM	Sistema operativo para PC IBM que puede aprovechar el microprocesador de 32 bits. Maneja multitareas y trabajo con redes.
Windows CE	Microsoft	Versión reducida del sistema operativo Windows para computadoras de mano y dispositivos de comunicación inalámbrica.
UNIX	AT&T, Santa Cruz OS	Se usa en PC potentes, estaciones de trabajo y minicomputadoras. Maneja multitareas, procesamiento multiusuario y trabajo con redes. Se puede trasladar a diferentes modelos de hardware de computación.
LINUX	Linux Torval y otros	Alternativa gratuita y confiable a UNIX y Windows NT y 2000 Server opera en muchos tipos distintos de hardware de computación y ofrece código fuente que los encargados de desarrollar software pueden modificar.
MAC OS	Apple Computer	Sistema operativo para la computadora Macintosh. Maneja trabajo con redes y multitareas, y cuenta con potentes funciones multimedia. Apoya la conexión a Internet y la publicación en ella.
DOS	IBM	Sistema operativo para PC IBM (PC-DOS) y compatibles con IBM (MS-DOS). Limita el uso de memoria de los programas a 640 K.
Solaris	Sun Microsystems	El UNIX de Sun Microsystems

Nota: Principales sistemas operativos. Fuente: (Amaya A. J., 2009)

1.3.3.1.2 Software de aplicación. Este término “describe los programas que se escriben para los usuarios o son escritos por ellos con el fin de aplicar la computadora a una tarea específica, los programadores que escriben software de aplicación se llaman programadores de aplicaciones”. (Amaya A. J., 2009, pág. 15). Así el software se aplica a cada una de las necesidades de las organizaciones que lo requieren de acuerdo a las características, entorno y medio en el que se desarrollan con fin de obtener el resultado deseado.

1.3.4 La información

Es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones (Chiavenato, 2006, pág. 18).

Un concepto válido para definir la información puede ser, “Como un conjunto de datos necesarios para la realización de uno o varios procesos, que organizados de una determinada manera, nos aportan un conocimiento de las cosas en general”. (De Pablos, Lopez Hermoso, Martin Romo, & Sonia, 2004, pág. 23).

En conjunto las dos definiciones podemos tener un concepto adecuado a nuestro tema de investigación, es un conjunto de de datos que se relacionan entre sí, organizados de distinta manera en un determinado contexto para su uso posterior e inmediato que nos permiten tomar acciones con respecto a la toma de decisiones.

1.3.4.1 Características de la información. La información se puede describir de dos maneras así:

A la información se la puede definir como un proceso mediante el cual alguien resulta informado, un proceso en el cual la emoción, el estado de ánimo, la predisposición, las expectativas, o la química entre el que

informa (informador), y quien es informado son decisivas en las respuestas cognitivas del informando, esta definición puede ayudarnos mucho a la hora de entender la información y en el diseño de sistemas de información, cada persona tiene características bien diferenciadas a la hora de procesar una información: lectura, selección, ordenación, interpretación, aplicación y esto nos lleva a anticipar aquí la necesidad de construir sistemas de información lo mas personalizados posibles. Desde esta perspectiva existen dos formas de entender la información una técnica y otra desde una perspectiva psicológica, la primera como un conjunto de señales o bits que viajan desde un emisor a un receptor a través de algún medio o canal.

La segunda manera de entender la información parte de dos mundos uno físico donde se producen los hechos que se traducen en datos concretos (la riqueza de un país, su capital, la cultura.) pero para que esos datos la información debe entrar en el mundo mental de los humanos, esta información estructurada solo sirve a quien espera utilizarla, y además si queremos que esa información se convierta en conocimiento se necesita que la persona que la utilice tenga criterio para saberla interpretar. (De Pablos, López Hermoso, Martin Romo, & Sonia, 2004, pág. 23).

El proceso de información parte de una necesidad de ser informado es decir conocer de algún dato o hecho en particular, por lo tanto en la organización es importante identificar al recurso humano involucrado en el proceso de recolección de información en el que cada uno tiene funciones y no debe salirse de ellas para la correcta unión de los hechos que ocurren para posteriormente tomar decisiones.

La necesidad de planificar la información, puede calcular sus costes, presupuestarla o evaluarla y por tanto considerarla como un recurso valioso y costoso, para ello se describen las siguientes características de la información:

- a) Una información es difícil dividirla en partes diferenciadas.

- b) La información no se gasta con el uso, no se devalúa, sino que incluso mejora con el mismo.
- c) Una información puede tener valor hoy y carecer del mismo mañana, la evolución en el tiempo del valor de la información es difícilmente previsible.
- d) La información puede ser de inmenso valor para un sujeto sin relevancia para otro, por tanto la información tiene valor en función de quien la use.
- e) Para que una persona pueda apreciar el valor de una información, es decir si esta satisface sus necesidades debería de poder conocerla, en este punto es importante dar a conocer que si la información que una persona necesita aun no la conoce o no tiene una noción de ella simplemente no tiene un valor en ese instante, sino después de haber indagado y buscado mas información que le permita tener un conocimiento más técnico y científico de aquello que necesita conocer.

De la observación de estas características se desprende la particularidad de este recurso hace que la forma de gestionarlo sea distinta a la manera de administrar y valorar otros bienes materiales, mercancías o recursos tradicionales de una empresa.

1.3.4.2 Cualidades de la Información

Hoy en día en la sociedad la información no es recurso escaso sino el tiempo, cada vez los directivos de las empresas tienen cada vez más información pero no tienen tiempo para procesarla, evaluarla y aplicarla por lo que la calidad de esta se convierte en un aspecto sumamente primordial y de especial significancia. (De Pablos, López Hermoso, Martin Romo, & Sonia, 2004, pág. 26)

A continuación se detallan las cualidades que debe tener la información para que esta sea de calidad de acuerdo a las siguientes características:

- a) **Relevancia.** Que la información se adecue a las necesidades del usuario, relevante para el Propósito de la decisión o del problema considerado.
- b) **Adecuación.** Que trate sobre el tema requerido.

- c) **Precisión.** Que de exactamente lo que se pide de ella.
- d) **Exhaustividad.** Lo importante es que la información sobre los elementos claves sea completa.
- e) **Fiabilidad.** Que la información sea cierta, que se confíe en la fuente de procedencia.
- f) **Puntualidad.** Que lo haga en el momento que necesite el usuario ni antes ni después.
- g) **Nivel de detalle.** Ni excesivo ni insuficiente.
- h) **Formato.** Que la presentación de la información, sea de manera textual, gráfica, o combinada responda a las expectativas del usuario.
- i) **Comprensibilidad.** Debe ser entendida por quien la vaya a utilizar.
- j) **Comunicabilidad.** Debe ser transmitida por el canal adecuado.

1.3.5 Las Bases de Datos. “Fondo común de la información almacenada en una computadora para que cualquier persona o programa autorizado pueda acceder a ella, independientemente de su procedencia y del uso que se haga.” (Pons Capote, Marín, Medina, Acid, & Vila, 2009, pág. 27). Este concepto nos habla de la posibilidad de compartir información entre los diferentes usuarios, además tiene que ser necesaria para los usuarios y los programas es el soporte para la implantación de bases de datos y que además tienen un carácter de información compartida es decir debe tener acceso restringido por parte de los usuarios y programas a la información de acuerdo a privilegios de acceso.

1.3.5.1 Sistema de gestión de bases de datos. “Es un conjunto de elementos de software con capacidad de definir, mantener y utilizar una base de datos”. (Pons Capote, et al. 2009, pág. 7). Es decir una base de datos es un elemento de un sistema de gestión de base de datos de esta manera podemos identificar como está estructurada y cuál es su contenido pero no como se crea, de tal forma se identifican las siguientes operaciones que debe de proveer un sistema de gestión de base de datos:

- a) Crear, modificar, eliminar, y obtener la estructura asociada al esquema lógico de una base de datos.

- b) Instanciar datos operativos en una base de datos, modificar dichas instancias, eliminarlas y recuperarlas bajo diferentes criterios de búsqueda.

1.3.5.1.1 Objetivos de un sistema de gestión de base de datos. A continuación presentamos 3 objetivos que debe satisfacer un sistema de gestión de base de datos:

Diseño y utilización orientada al usuario. Los datos y las aplicaciones deben estar accesibles a los usuarios de la manera más amigable posible. Para ello los sistemas de gestión de bases de datos habrán de fundamentarse en un modelo de datos teórico coherente y proporcionar lenguajes que permitan definir la estructura de la Base de Datos y acometer la generación, mantenimiento y acceso a los datos en los términos que resulten apropiados.

Centralización. Los datos deben gestionarse de forma centralizada e independiente de las aplicaciones para satisfacer este objetivo un sistema de gestión de base de datos habrá de proporcionar una serie de utilidades que facilitan la administración de ese fondo común. Adicionalmente aparece la figura del administrador de base de datos como responsable de las tareas que permitan mantener la disponibilidad de ese fondo común.

Evitar la redundancia y gestionar la concurrencia. El sistema de gestión de base de datos provee un fondo común de datos que puede ser compartido por varias aplicaciones, no es preciso, por tanto duplicar dicha información, sin embargo puesto que varias aplicaciones pueden acceder a los mismos datos al mismo tiempo, el sistema de gestión de base de datos debe disponer de los mecanismos adecuados para gestionar esas concurrencias.

Por tanto es necesario conocer primordialmente las necesidades de la organización y que información desea que esté disponible, la misma que debe tener acceso restringido de acuerdo a parámetros de acceso, estructurada de tal manera que se la pueda crear, modificar, eliminar en un cualquier momento sin que existan concurrencias en este proceso.

1.3.6 Las redes de comunicaciones

Para iniciar se detallan las diferentes formas tecnológicas de conectividad de las empresas y se describen en principio los tipos de señales, existen dos formas de comunicar un mensaje: mediante una señal analógica y una señal digital. Una señal analógica se representa por medio de una onda continua que pasa a través de un medio de comunicaciones y ha sido utilizada para la comunicación de voz. Los dispositivos analógicos más comunes son el auricular del teléfono, la bocina de una computadora o los audífonos de un ipod, estos crean formas de onda analógicas que su oído puede captar. Una señal digital es una forma de onda binaria, discreta, en vez de continua, las señales digitales comunican la información como cadenas de dos estados discretos uno y cero bits, los cuales se representan como pulsos eléctricos de encendido-apagado. (Laudon, 2008, pág. 269).

1.3.6.1 Tipos de redes. Existen muchos tipos de redes y formas de clasificarlas a continuación se muestra una manera de considerar las redes por su alcance geográfico la siguiente tabla nos muestra estos tipos:

Tabla 2.
Tipos de Redes

TIPO	ÁREA
Red de área Local (LAN)	Hasta 500 metros media milla; una oficina o un piso de edificio
Red de área de Campus (CAN)	Hasta 1000 metros una milla; el campus de una universidad o las instalaciones de una corporación.
Red de área metropolitana (MAN)	Una ciudad o un área metropolitana.
Red de área Amplia (WAN)	Un área transcontinental o mundial.

Nota: Tipos de redes que actualmente se encuentran disponibles.

Para simplificar de manera más concreta las LAN conectan computadoras de una oficina un o un negocio, cuando se unen las redes LAN de un conjunto de oficinas se convierten en CAN ejemplo un edificio de oficinas o un campus universitario, las redes MAN conectan a un sitio geográfico en particular como una ciudad o un distrito, las redes WAN se conectan entre redes públicas mas grandes a través de la utilización de redes de satélites o líneas telefónicas de manera más global.

1.3.7 Las personas (Usuarios)

En primera instancia se distingue dos tipos de recursos humanos dentro del sistema de información de una empresa: los usuarios finales y el personal propio de dichos sistemas así:

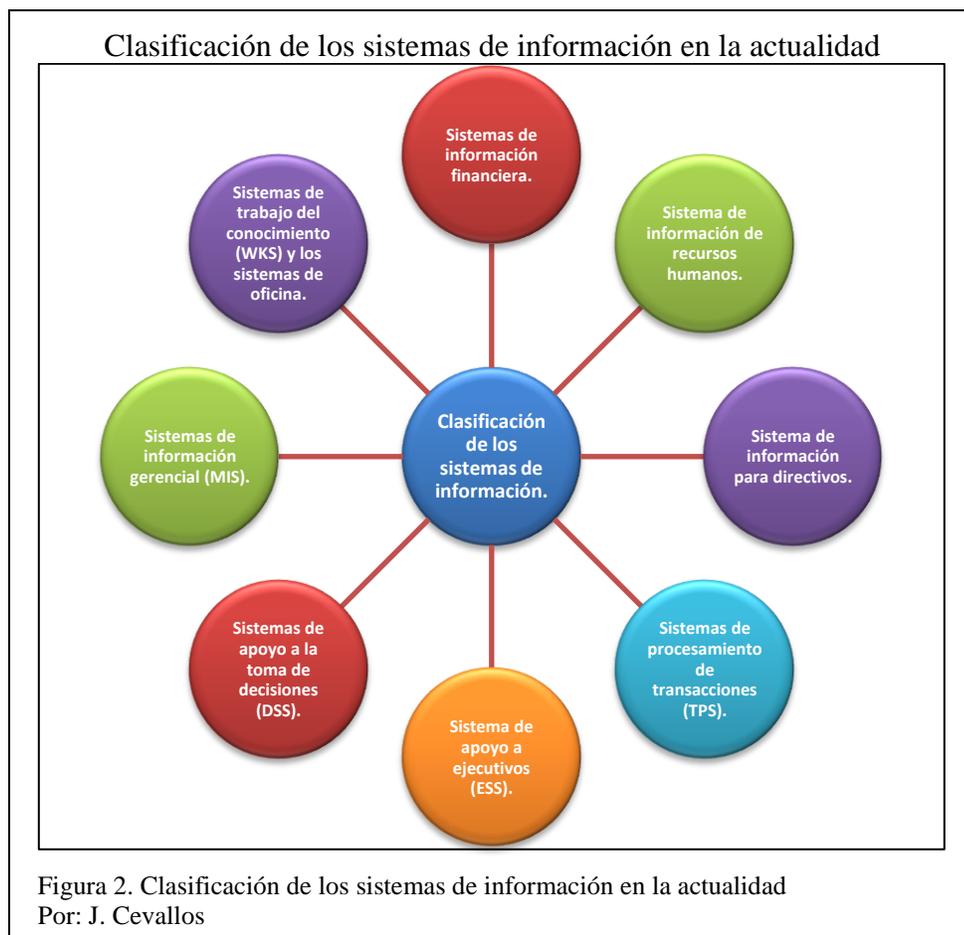
Los usuarios finales son todas aquellas personas que participan en el sistema de información de una empresa para obtener su producto final, podemos considerar que todos los miembros de una organización son potencialmente usuarios finales del sistema, ya que todos ellos van a necesitar utilizar y/o modificar la información. El papel de los usuarios finales de los sistemas de información ha tomado una mayor relevancia en los últimos años, debido sobre todo a la descentralización de dichos sistemas, de este modo cada vez una proporción mayor del personal de una organización determinada se ve involucrada no solo en el tratamiento de la información y la obtención de un resultado, sino en otras actividades, como puede ser el desarrollo de sistemas. Y la división del personal de sistemas de información en función del escalón jerárquico de responsabilidad en el que se sitúan, podemos considerar de esta forma, que el sistema incluye un alto ejecutivo de la compañía, el CIO (Chief Information Officer – Gerente de la información), dependiente de muchos casos directamente del presidente o director general de la empresa, un cierto número de directivos intermedios, con ciertos número de responsabilidades limitadas, el personal técnico, especializado en determinadas tareas de un cierto valor añadido par al empresa, y por tanto un cierto margen de decisión; y el personal de operaciones, encargado de la realización de las tareas concretas de carácter estructurado, esto es con poca autonomía. (De Pablos, Lopez, & Santiago Martín-Romo, 2006. pág. 24).

Simplificando la definición anterior se tiene a los usuarios finales quienes sacan provecho de la información que se obtiene como producto final del uso apropiado de

los recursos, la capacidad de tomar decisiones y por supuesto la manera que la información fue tratada hasta que llegó a manos de los directivos para que puedan analizarla e implementar planes de acción, y esta va de la mano con el personal de los sistemas de información, que va desde el director ejecutivo, directivos intermedios, personal técnico y personal operativo encargado de la realización de tareas, con base a los lineamientos que necesita la organización.

1.4 Clasificación de los sistemas de información

En la actualidad existen muchas clasificaciones para los sistemas de información, de acuerdo a las necesidades de la organización y en base a los objetivos que desea cumplir para que resulten más eficientes al obtener los datos y permitan disponer de los mismos en cualquier instante, por lo tanto (Fernández, 2006, pág. 24) los detalla así:



Sistemas de información financiera. Este sistema de información es de gran importancia y es el más utilizado por las organizaciones les permite controlar la información que ingresa esta al ser transformada a un valor monetario se la puede proyectar y presupuestar a corto y largo plazo, también existe la capacidad de regular todos los procesos financieros que se realizan por medio de los directores quienes son los encargados de controlar estos procesos.

Sistema de información de recursos humanos. A través del sistema de recursos humanos podemos identificar con claridad el recurso humano que va a laborar en la empresa, su información contable, crediticia, su experiencia, identifica al trabajador donde va a trabajar, cuáles son sus funciones, cuáles son sus beneficios, pero también nos permite medir el desempeño la eficiencia del trabajador en la operaciones de la organización en base a indicadores, que nos muestren sus competencias de manera general y específica.

Sistema de información para directivos. Proporciona a un directivo información sobre el desempeño global de la empresa, estos sistemas utilizan fuentes de información interna de la propia organización y fuentes provenientes del entorno ya que la información proviene de los niveles jerárquicos más altos.

Sistemas de procesamiento de transacciones (TPS). En este tipo de sistemas se pueden encontrar procesos repetitivos pero que en realidad si se los aplica desde un sistema informático adecuado, puede eliminar tiempos de espera y hacer que cierto tipo de operaciones se desarrolle de manera programada, por lo tanto, se incrementa la capacidad productiva de las operaciones.

Sistemas de trabajo del conocimiento (WKS) y los sistemas de oficina. Este tipo de sistemas permite integrar la comunicación de las diferentes áreas de la organización, como por ejemplo al realizar un diseño de un nuevo producto se lo pasa por el departamento creativo, luego espera su procesamiento en el de producción, si es favorable, espera su aprobación por la gerencia, por tanto este proceso está integrado entre sí y permite la interrelación entre los departamentos a través de ordenes de entrada y salida, preparación procesamiento de pedidos, los

mismos que se basan en sistemas de oficina orientados a maximizar los resultados y el tiempo de espera por procedimiento.

Sistemas de información gerencial (MIS). Los sistemas de información gerencial (MIS) nos presentan una información poco flexible es decir que no se pueden hacer cambios o modificaciones en los datos, porque en el informe ya está resumido por lo tanto se tiene una concepción en general con respecto a los hechos registrados por parte del sistema de procesamiento de transacciones.

Sistemas de apoyo a la toma de decisiones (DSS). Este tipo de sistemas permite tomar acciones cuando aparezcan imprevistos o situaciones que no sean muy comunes en la organización, por tal motivo también se adaptan y permiten generar nuevas oportunidades para la toma de decisiones así como el mejoramiento y la optimización de recursos de ser necesario, por tanto es necesario tener una estrategia adecuada que maximice la capacidad de la empresa para enfrentar problemas.

Sistema de apoyo a ejecutivos (ESS). El (ESS) es un sistema apropiado para ejecutivos de mandos altos que necesitan la información de tal forma que se la pueda manipular y se pueda crear proyecciones de valor a largo plazo, su importancia radica en el momento que permite reconocer posibles amenazas o debilidades de la empresa, permiten contar con una herramienta objetiva que se basa en datos actuales y dirige sus fortalezas para aquellos puntos que necesitan más atención y contrarrestar los efectos de una posible situación de conflicto.

1.5 Fases en el desarrollo de sistemas de información

Existen 4 fases en el desarrollo de sistemas de información como lo detalla (Fernández, 2006) en su libro así:

- a) Planificación de sistemas
- b) Análisis de sistemas
- c) Diseño de sistemas
- d) Implantación y soporte de sistemas.

1.5.1 Planificación de sistemas. “Es un plan estratégico que nos proporciona la dirección correcta en el desarrollo de sistemas, el modo de proceder, los criterios de selección, los mecanismos de evaluación, etc.” (Fernández, 2006, pág. 49). Esta planificación permite conocer en primera instancia los lineamientos que se necesita para poder iniciar a desarrollar la posible implementación de un sistema de información, de tal forma que es necesario tener un conocimiento previo de las necesidades de la organización y partiendo de este punto se puede desarrollar el plan con las estrategias necesarias.

Para continuar con el proceso de planificación se tienen en cuenta siete pasos que permiten continuar hacia el cumplimiento de los objetivos de la organización y que los describe (Fernández, 2006, pág. 54), en su libro y se los plantea así:

- a) Seleccionar a los participantes en el desarrollo de un sistema
- b) Definir los objetivos y alcance del proyecto.
- c) Definición de actividades.
- d) Asignar recursos.
- e) Planificar un calendario.
- f) Diseñar criterios de evaluación.
- g) Estudiar la viabilidad del proyecto.

Es necesario considerar que al seleccionar los participantes debe ser un personal entrenado y capacitado para el proceso de desarrollo de sistema, el mismo que debe tener la experiencia y el suficiente conocimiento científico para desarrollar sus actividades.

Al definir los objetivos del proyecto se debe tomar en cuenta hasta dónde quiere llegar la organización, a qué instancia desea llegar por ejemplo el posicionamiento de mercado, lanzamiento de una nueva marca que tenga atractivo en más del 50% de la población, etc. Por tal motivo es necesario conocer si los recursos que posee son los suficientemente necesarios para conseguir los objetivos.

Para definir las actividades se debe primero definir las competencias de cada uno de los participantes, de ahí delimita la función de cada uno, que procedimientos va realizar en el proceso de diseño y como en su conjunto con los participantes cumplen con las metas establecidas.

A través de la asignación de recursos se tiene en cuenta lo materiales, el recurso humano, tecnológico, financiero que se necesita para el desarrollo de un sistema el mismo que se basa en plazos y tiempos establecidos, a través de un presupuesto debidamente analizado, aprobado y controlado de manera eficiente permitirá la consecución de las tareas con normalidad y de acuerdo a los parámetros establecidos para cada uno.

Se debe tener en cuenta un calendario de actividades en el que cada cierto tiempo tiene que hacerse revisiones y seguimiento del avance de las tareas que se están realizando, esto exige un control que previene en ciertos casos la demora de los procedimientos a realizarse y se puede tomar medidas preventivas para cumplir con el calendario.

Para diseñar criterios de evaluación es necesario conocer todas las operaciones que se van a realizar y la calidad de las mismas porque depende mucho del grado de confiabilidad que tiene cada procedimiento, cuando es ejecutado en el proceso, cuando se mide su grado de eficiencia y operatividad al momento de ejecutarse y como consecuencia se debe tener una valoración positiva para continuar con el proyecto.

Y por último para estudiar la viabilidad del proyecto es necesario considerar todos los pasos antes mencionados y si cumplen con el mínimo de calificación en los controles entonces se lo aplica pero también se tiene en cuenta la implicación que tiene también en las políticas de la organización, es decir si esta aprobado para que en el momento que deba ser implantado, se lo pueda realizar con total normalidad.

1.5.2 Análisis de sistemas de información

En este punto “el enfoque se centra en aspectos del negocio, más concretamente con las necesidades y objetivos de los propietarios y los usuarios de sistemas, este análisis de compone de dos fases: análisis del sistema actual y análisis de requerimientos o necesidades.” (Fernández, 2006, pág. 70). Para el estudio del sistema actual se toma en cuenta las fortalezas y las debilidades para conocer la capacidad operativa que mantiene en este momento, que partes del sistema se pueden salvar, sacar respaldos, información que nos permitirá en primera instancia conducirnos hacia los objetivos de la empresa. Por otra parte también es necesario analizar los datos que nos proporcione el actual sistema y dependiendo para el área al que pertenece dicha información porque puede contener información de tipo confidencial y sensible, por ejemplo del área de recursos humanos, tesorería, comercio exterior, cartera vencida, inventarios, etc. Otro punto importante es cómo se maneja por separado, entonces depende de la capacidad del análisis separar por grupos la información y coordinar con el jefe de cada área para iniciar con el proceso de análisis-revisión-eliminación, de aquellos datos que realmente no están en función del área al que pertenece, por ultimo tener listo toda lo que es importante y necesario para la organización y después en la implantación migrar los datos al nuevo sistema.

La actividad que se realiza en esta etapa es “la estructuración de los requisitos funcionales, el objetivo de esta actividad es exponer los requisitos de forma comprensible a los usuarios y a los propietarios para que puedan verificarlos y aprobarlos.” (Fernández, 2006, pág. 85), de esta manera una vez conocidas las necesidades de la organización, analizado y estudiado las propuestas se procede con la aprobación de los usuarios y de los propietarios confirmando así los procesos a seguir en el diseño de sistemas en donde se plasma los requerimientos para que puedan ser utilizados por los usuarios.

Además del proceso detallado anteriormente se debe tomar en cuenta los siguientes puntos:

Entrevistas. “Es necesario que los analistas se reúnan con los clientes del sistema y demás personas involucradas con el mismo a fin de conocer cuáles son sus inquietudes y requerimientos.” (Amaya A. J., 2009, pág. 110). En este punto se debe conocer todas aquellas necesidades que se deben tomar en cuenta con prioridad, para la solución del problema y las causas que la originaron para poder incluir en la base de datos con fin de reunir toda la información que determinará todos los pasos a seguir en el proceso de análisis.

Encuestas. “Una vez realizadas las entrevistas se debe proceder, en la mayoría de los casos, y cuando se amerite, a desarrollar y aplicar encuestas que busquen hacer una investigación de mercado entre los futuros clientes del sistema.” (Amaya A. J., 2009, pág. 110). En las encuestas es necesario conocer cuáles son las expectativas, lo que necesita la organización en materia de obtener información ya sea oportuna, por periodos o simplemente dependiendo del nivel jerárquico se puedan utilizar atributos para cada uno por tanto también se puede incluir el nivel de seguridad.

Manuales y Procesos. “Los manuales de procesos son herramientas de primera mano para saber en detalle que es lo que se quiere sistematizar.” (Amaya A. J., 2009, pág. 110). Es necesario que el analista o el grupo de trabajo conozcan los procedimientos porque a través de ellos se puede encaminar hacia el diseño del sistema y éste satisfaga los requerimientos de cada uno de los manuales que puedan tener, ya sea por área por proceso o por usuario.

Los documentos. “Es necesario que el analista recolecte y analice todos los documentos necesarios para involucrarlos en el proyecto de sistematización.” (Amaya A. J., 2009, pág. 110). Una vez realizados los pasos anteriores dependiendo de la capacidad del analistas puede crear nuevos documentos, hacer diagramas tablas, figuras donde se incluyan todos los datos recolectados de tal manera que estén disponibles de manera concatenada para el proceso de diseño de sistemas.

1.5.3 Diseño de sistemas de información. “Es el plan o modelo general del sistema, se detalla las funciones que se implementarán y están identificadas en la fase de análisis, todas estas especificaciones deben contemplar los componentes de

administración, organización y tecnología del sistema de solución.” (Amaya A. J., 2009, pág. 111). Por lo tanto en esta fase se crea el modelo conceptual a implantarse en la organización de acuerdo a las especificaciones y funciones que se describieron en la fase de análisis y donde deben de constar todos los procesos para todas aquellas áreas o departamentos para el cual fue creado.

Para realizar el proceso de diseño se pueden utilizar:

1.5.3.1 Diagramas de contexto

Definen la interacción del sistema con el ambiente externo a él, compuesto por usuarios, clientes, otros sistemas, archivos, etc. y los diagramas funcionales son los que describen operaciones básicas del sistema que le permitirán cumplir con las tareas para las cuales fue diseñado y el diagrama de flujo de datos (DFD) describe como fluyen los datos a través del sistema mediante el esquema Entrada-Proceso-Salida. (Amaya A. J., 2009, pág. 111)

De esta manera se identifican los diferentes tipos de diagramas a utilizar según la necesidad de la empresa para cada tipo de proceso, por tanto se enlazan y permiten la interrelación de datos, resulta necesario para que en cualquier momento se puedan hacer las pruebas y se puedan verificar si todos los puntos a los que se conectan puede obtener la información completa o parcial, y si estos datos están disponibles en cualquier momento.

A partir de este punto se puede aplicar una técnica de “Modelo de entidad relación es la técnica que permite definir los datos, es decir, las entidades sus atributos y las relaciones entre las mismas” (Amaya A. J., 2009, pág. 111). En este modelo define los niveles de acceso y se identifican los usuarios que pueden ingresar al sistema, también se definen que tipo de acciones que realizan y están autorizados a ejecutar.

Existen dos fases para el diseño y estas son:

1.5.3.1.1 Fase de diseño lógico del sistema

Se basa en que funciones lógicas se puede implementar en el sistema sin tener en cuenta ningún tipo de tecnología, por tanto permite que el analista de sistemas se centre más en las necesidades de la organización y utiliza este diseño para estructurar y documentar los datos esenciales del negocio y no le presta mucha atención al elemento tecnológico ya que puede omitir algún requerimiento o necesidad funcional. (Fernández, 2006, pág. 91)

Este punto se centra más en buscar satisfacer todos los puntos que la organización que necesita que sean atendidos, aquellos temas que se necesita controlar y superar con el sistema y que se pueda dar opciones de solución en cualquier momento.

1.5.3.1.2 Fase del diseño físico del sistema

Se centra en los aspectos técnicos y de implementación del sistema de información, a diferencia del diseño lógico que se centra en aspectos del negocio, a partir de este punto existen dos opciones para la implementación: la primera es implementar internamente el sistema de información que se ha analizado y diseñado, o implementar el sistema de información a través de agentes externos, en este caso también existen dos opciones: subcontratar a una empresa externa para que realice el diseño físico del sistema y lo implemente según el diseño lógico que se ha desarrollado o comprar un sistema de información estandarizado. (Fernández, 2006, pág. 91)

En esta parte del diseño es importante recalcar que al realizar el diseño físico del sistema el equipo ya tiene la capacidad de crear el diseño físico, caso contrario en el momento en que se encuentren con una dificultad pueden contratar un asesoramiento

y de ser el caso de mejor manera subcontratar a una empresa para que realice el diseño físico en base al diseño lógico que ya se detalló con anterioridad.

1.5.4 Implantación y soporte de sistemas

Esta es la última etapa en el proceso de creación de un nuevo sistema de información y que es la unión de los pasos y procedimientos detallados en el diseño del sistema, es en este momento donde se instala, conecta con los medios físicos se prueba y se evalúan los errores encontrados que puedan existir, para luego corregirlos y poner en marcha al sistema, en cuanto al soporte pues el analista y la persona que monitorea el sistema deben brindar su ayuda cuando los usuarios lo requieran o cuando exista un conflicto usuario-software o viceversa o también conflictos con los medios físicos que apoyan al nuevo sistema de ahí que el soporte debe ser antes durante y después de la utilización.

1.5.5 Importancia de los sistemas de información

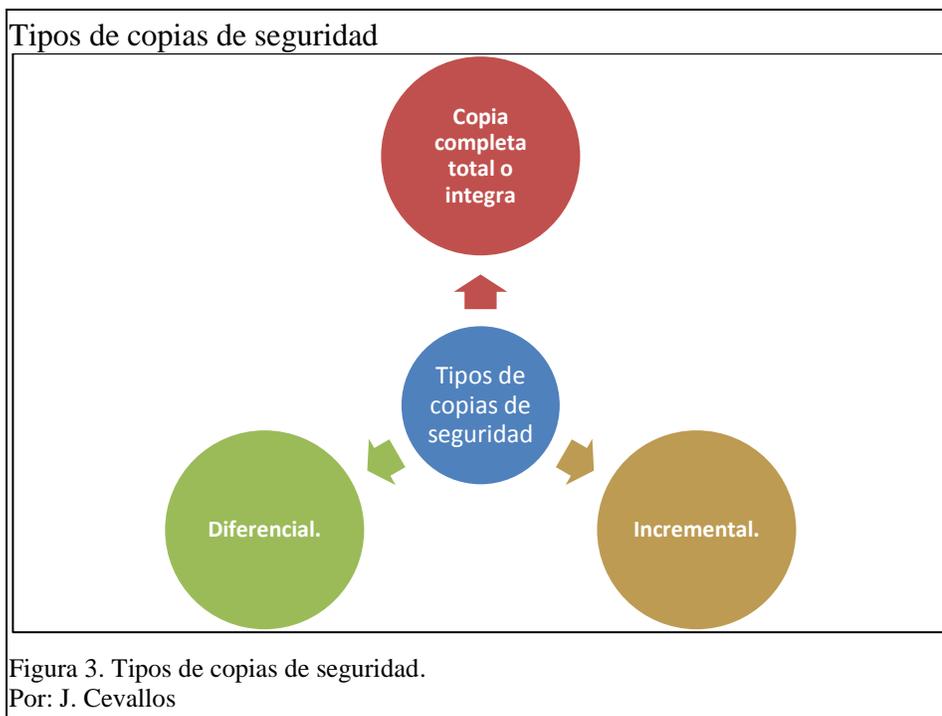
Desde un enfoque organizativo, el sistema de información se relaciona con todas las actividades que se desarrollan en la empresa y éstas dependen en su mayoría, aunque de modos diferentes, del sistema. Por tanto los cambios en los sistemas de información alteran la dinámica de la organización y viceversa. (De Pablos, Lopez, & Santiago Martín-Romo, 2006, pág. 106)

El sistema de información es importante en la medida de que todas las actividades de la empresa dependen de él entre sí, es decir, con la ayuda del software tecnológico y en unión a los medios físicos se pueden integrar procesos y recursos que permiten utilizar al máximo el elemento más importante que tiene la empresa y que es la información.

1.6 Copias de seguridad (backups). “Son copias de la información de un sistema informático de tal forma que pueda ser recuperada en cualquier momento en el caso de que falle, se borre accidentalmente o simplemente porque ocurrió algún tipo de

contingencia.” (Garcia-Cervigón Hurtado & Alegre Ramos, 2011, pág. 60). Analizando este concepto es necesario dar a conocer que siempre se necesita copias de seguridad de la información que se está utilizando, porque siempre pueden ocurrir imprevistos como por ejemplos desastres naturales, mal manejo de los recursos físicos de la organización, o descuido en el mantenimiento de las instalaciones eléctricas puede ocasionar que se pierda de forma parcial o total la información, de esta forma “Antes de decidir hacer las copias de seguridad es necesario también conocer en que medio se lo va realizar, es decir en una cinta magnética, en otro disco duro, ya sea interno o externo, mediante una unidad extraíble USB, en una memoria flash o un pendrive”. (Garcia-Cervigón Hurtado & Alegre Ramos, 2011, pág. 60) y si se utiliza alta cantidad de información se debe utilizar un servidor externo que realice copias de seguridad continuamente para no tener pérdida de la información.

Otro punto importante que es necesario conocer es que tipo de copias de seguridad se va a realizar, existen tres tipos como lo muestra (Garcia-Cervigón Hurtado & Alegre Ramos, 2011) en su libro así:



Copia completa total o integra. Copia todos los archivos y directorios que se desea respaldar.

Incremental. Copia todos los archivos que se hubieren modificado desde la última copia de seguridad, esta puede ser incremental o completa.

Diferencial. En este caso copia todos los archivos que se modificaron a partir de la última copia de seguridad completa.

Al realizar estos procedimientos nos permite obtener la información que necesitamos en cualquier momento, por ejemplo en la copia total señalamos todos los archivos que queramos respaldar, en la copia incremental podemos restaurar la información desde la última copia de seguridad realizada pero de los archivo que se han modificado pro existe la opción de restaurar todas las copias incrementales que se realizaron con posterioridad, y para finalizar la diferencial que se puede recuperar la información a partir de la modificación de los archivos de la ultima copia de seguridad completa.

Otro punto importante es que también podemos comprimir la copia de seguridad para que ocupe menos espacio y lo que se debe hacer es automatizar el proceso para que en ningún momento se pierda la información.

Imágenes de respaldo. “Es la copia de seguridad de todo el sistema, en estas imágenes solo se copia los archivos modificados últimamente, sino también todo el disco duro mediante un fotografía, se almacena para posteriormente ser repuesta en caso de fallo”. (Aguilera López, 2010, pág. 201). En este caso las imágenes de respaldo se las puede utilizar en caso de que un equipo pueda fallar con frecuencia o tiene una infección por virus por lo tanto se debe instalar de forma adecuada software y sistemas operativos que eviten el fallo de los equipos y estén siempre disponibles y seguros.

1.6.1 Planes de contingencia. “Es una herramienta de gestión que nos permite conocer las acciones (tecnológicas, humanas y de la organización) para que se pueda garantizar la continuidad del negocio protegiendo los sistemas de información tras

algún incidente de causa accidental o de manera natural.” (Aguilera López, 2010, pág. 23). El plan es una herramienta importante a la organización para continuar con el negocio porque le permite estar preparado en caso de desastres naturales, pérdida o daño de la información, lo mejor opción es tener un plan para recuperar la información y como se la va a utilizar posteriormente porque siempre puede existir la probabilidad de que pueda ocurrir un nuevo incidente.

Existen tres tipos de planes de contingencia que se deben tomar en cuenta y que los detalla (Aguilera López, 2010, pág. 23) en su libro de la siguiente forma:

1.6.1.1 Plan de respaldo. En este plan se toman medidas para evitar que se produzca un daño a la información.

En este plan se realizan pruebas y simulacros de lo que podría pasar en caso de que un siniestro pueda ocurrir en la organización y como se puede actuar y en qué lugar se puede tener un respaldo de la información.

1.6.1.2 Plan de emergencia. Son las acciones que se debe tomar en el instante en que está ocurriendo un evento inesperado.

En este tipo de plan se ejecutan los procedimientos en tiempo real por ejemplo que se realicen las copias de seguridad automáticamente, y que toda la información se envíe a los servidores de respaldo.

1.6.1.3 Plan de recuperación. Se aplica todos los procedimientos que se deben seguir después de que ha ocurrido un desastre.

Dependiendo del tipo de daño si las instalaciones actuales no brindan la seguridad adecuada se debe tener un edificio de operaciones temporal, de tal forma que se pueda continuar con las operaciones y obtener toda la información respaldada en los medios adecuados para su uso.

El plan de contingencia debe contener un conjunto de elementos necesarios para que su implantación sea la adecuada y las detalla (Echenique García, 2004, pág. 263) en su libro de la siguiente forma:

- a) Señalamiento de los procesos críticos.
- b) Su impacto
- c) Prioridad
- d) Tiempo en el que se puede estar fuera de línea con el sistema
- e) Información existente de cada proceso.
- f) Documentación para la recuperación.

Además por cada usuario debe tener la siguiente información:

- a) Software
- b) Hardware
- c) Recursos materiales
- d) Personal
- e) Utilerías
- f) Sistemas de comunicación
- g) Redes
- h) Transporte
- i) Bases de datos
- j) Archivos (respaldos).

Es necesario que la organización siempre esté en constante innovación con respecto al manejo de la información para que pueda hacer frente a los incidentes que se puedan suscitar, tener en cuenta que realizar este plan conlleva un gasto en recursos materiales, económicos y humanos pero a mediano y largo plazo resultan para la organización un alto beneficio en materia de seguridad.

1.6.2 Herramientas de respaldos automáticos

Las herramientas para realizar respaldos automáticos permiten realizar copias de seguridad de los datos que se desea guardar por ejemplo en Windows la herramienta predeterminada por el sistema es copias de seguridad y restauración que nos permite realizar múltiples opciones de respaldo y se las detalla así:

Copias de archivos personales. En esta opción permite realizar copias de seguridad de archivos de trabajo, documentos, imágenes, videos en una ubicación diferente a la original.

Copia de todos los archivos del equipo. En este caso Windows crea una imagen con toda la información almacenada en el equipo como por ejemplo archivos personales, programas y archivos del sistema.

Archivos del sistema. Este tipo de copia de seguridad lo administra Windows mediante puntos de restauración, es decir que de forma automática realiza una copia de archivos del sistema cuando un programa modifique dichos archivos, también se lo puede realizar de manera manual un punto de restauración..

Algunas empresas que implementan software se dedican al desarrollo de nuevos programas que permiten realizar copias de seguridad en base a cada una de las necesidades de las organizaciones dependiendo del entorno de trabajo, recursos tecnológicos e infraestructura que posea, algunas de las empresas que fabrican este tipo de software son Acronis, Nanosystems S.r.l., y Symantec entre otras a continuación se detalla alguno de sus productos de las mismas así:

Acronis true image. Este programa realizar imagen del sistema operativo, controladores programas, la imagen que genera o la copia de seguridad se puede guardar en otra partición del disco, otro disco, un disco externo o incluso hasta en la nube a través de la aplicación Acronis Cloud. (Acronis, 2014)

Unarium backup free. Es la solución para realizar copias de seguridad de fotos y videos, documentos comerciales y todo aquello que el usuario desea proteger que incluye una herramienta de planificación completa con sistema de informe completo vía correo electrónico. (Nanosystems S.r.l., 2014)

Norton ghost 15.0 Herramienta que permite realizar copias de seguridad de todo el sistema, copias de seguridad incrementales, diferenciales, copias de seguridad granulares (archivos, formatos o carpetas), copias de seguridad cuando se instala un programa, se pueden codificar la copias para brindar más seguridad y por último se puede realizar respaldos en cd, dvd, usb y formato zip. (Symantec, 2014).

1.7 Políticas de seguridad

En la actualidad para manejar la seguridad de la información existe un conjunto de normas de calidad llamadas ISO-17799, estas permiten la administración de todos los datos de la organización de manera segura y se basan en los siguientes objetivos:

Política de seguridad corporativa para todo el personal. Conformar todos los procesos y procedimientos a seguir de todos los miembros de la organización para el manejo de la seguridad de la información.

Organización de la seguridad. Se encarga de organizar la seguridad para los diferentes usuarios es decir los niveles de acceso que tiene cada persona.

Control y clasificación de activos. Establece los controles para el hardware y software de la compañía como un recurso esencial y propio de la organización. (Areitio, 2008, pág. 90)

La ISO -17799 contiene un conjunto de políticas estas son:

- a) Seguridad del personal
- b) Seguridad física y ambiental

- c) Manejo de comunicaciones de las operaciones.
- d) Control de acceso
- e) Desarrollo y mantenimiento de los sistemas.
- f) Manejo de la continuidad de la empresa
- g) Cumplimiento
- h) Políticas de seguridad.
- i) Organización de la seguridad.
- j) Control y clasificación de los recursos de la información.

Los beneficios de utilizar esta norma son los siguientes:

- a) Mejoramiento de la seguridad empresarial.
- b) Planeación más efectiva de la seguridad.
- c) Manejo más efectivo de la seguridad.
- d) Continua Protección
- e) Alianzas más seguras.
- f) E-commerce más seguro.
- g) Mayor confianza del cliente.
- h) Mayor Auditoría ROI
- i) Menor responsabilidad civil

1.7.1 Política de pólizas de seguros de equipo electrónico

Existen algunas pólizas para cubrir equipo electrónico de eventos que puedan ocurrir en la operación de la empresa, dependiendo del tipo de siniestro la aseguradora cubrirá los equipos siempre y cuando se cumplan las condiciones, a continuación presentaremos un ejemplo que detalla (Qbe Seguros Colonial.) En sus condiciones generales de equipo electrónico:

Cobertura. Todos los bienes asegurados en la parte descriptiva, sufrieren algún daño físico e imprevisto y que necesiten reparación o reemplazo la compañía indemnizara al asegurado tales pérdidas o daños.

Incremento en el costo de operación. Permite a la compañía cubrir gastos de operación que la empresa asegurada pueda tener por concepto de interrupción total o parcial de las operaciones en el sistema electrónico de procesamiento de datos especificados en la parte descriptiva.

Exclusiones. La compañía no indemnizará a la empresa asegurada los daños causados al equipo electrónico por:

- a) Guerra, invasión, acto de enemigo extranjero, rebelión, insurrección, motín, huelga, decretado por el empleador o grupos de personas maliciosas que puedan tener alguna conexión política con el asegurado.
- b) Reacción nuclear, radiación nuclear o contaminación por radiación.
- c) Acto intencional por parte de la empresa asegurada o sus representantes.
- d) Franquicias deducibles estipuladas en la póliza.
- e) Terremotos, temblor, maremoto, erupción volcánica, tifón, huracán o ciclón.
- f) Hurto o robo.
- g) Fallo en los equipos y que estos no sean conocidos por la aseguradora al momento de la suscripción del contrato.
- h) Fallo o interrupción del suministro de agua, gas o energía.
- i) Desgaste del equipo por las condiciones atmosféricas.
- j) Gastos para eliminar fallos operacionales.
- k) Partes desgastables como tubos, bandas, sellos, cintas etc.
- l) Defectos estéticos como raspaduras en la superficie del equipo.
- m) Restricciones impuestas por parte autoridades públicas en base a la reconstrucción y operación de equipo electrónico.

Suma asegurada. El valor de la suma asegurada es por el mismo valor del bien asegurado por otro nuevo de la misma clase.

Cambios que invalidan el seguro

- a) Cambio o modificación del edificio que contiene los bienes asegurados.
- b) Falta de ocupación del edificio por más 30 días.

- c) Traslado de los equipos a un lugar diferente de los señalados en la póliza.
- d) Traslado de dominio de los bienes asegurados, siempre y cuando se cumplan con los preceptos legales.

Pago de la prima. El pago de las primas son al contado y por anticipado pero también pueden existir facilidades de pago para pagar las cuotas.

Pérdida de beneficios. Los beneficios de la póliza se pierden sí:

- a) Los documentos firmados por la empresa asegurada existe falsedad o en los formularios de reclamación existe se hicieran reclamaciones falsas.
- b) Si el siniestro hubiese sucedido de manera intencional o con la intervención de un cómplice.

Pago de la indemnización. Si la empresa acepta una reclamación deberá pagarla dentro de los 45 días siguientes a la reclamación.

Endoso de la póliza. La póliza no podrá cederse o endosarse antes o después del siniestro sin previa autorización de la compañía.

Jurisdicción. La presente póliza solo será válida en el territorio ecuatoriano donde se encuentra domiciliada la empresa asegurada.

Prescripción. Los derechos, acciones y beneficios tendrán validez a partir de la fecha de la suscripción del contrato.

Seguridad del personal. Establece el marco de seguridad para el personal y como evitar la pérdida de la información ya sea por causa accidental por robo o fraude.

Seguridad física y ambiental. Este objetivo se concentra sobre el cuidado de las instalaciones así como la seguridad física del hardware de la compañía.

Administración de las comunicaciones y operaciones. Se refiere a la seguridad del software de la compañía en contra, de virus software malicioso, cambios en las copias de seguridad para obtener los soportes respectivos en caso de algún incidente.

Control de acceso a los sistemas. Corresponde al uso de contraseñas de seguridad para la autenticación de cada usuario y también el monitoreo del software de la compañía.

Desarrollo y mantenimiento del sistema. Consiste en la implantación de nuevos sistemas y la salvaguarda de los datos en caso de cambios, nuevas configuraciones y protección de los datos.

Gestión de la continuidad del negocio. Se encarga de ejecutar pruebas en todo el sistema de información para la seguridad de la información en caso de un siniestro y se pueda utilizar otra vez todos los datos respaldados.

1.7.2 Niveles de seguridad

A continuación se detallan los niveles de seguridad que debe existir en un sistema de información, estos son muy importantes ya que la falta de uno de ellos puede resultar peligrosa para la organización, porque lo que se busca es mantener todos los datos de la empresa seguros y con un mantenimiento adecuado.

1.7.2.1 Seguridad Física

El objetivo es establecer normas y procedimientos para evitar la interrupción del procesamiento de la información y estar siempre preparada la empresa para que pueda combatir los contingentes que se puedan suscitar (incendios, inundaciones, disturbios, robos, catástrofes naturales) y se pueda continuar con un medio de emergencia hasta que se normalice las actividades. (Echenique García, 2004, pág. 219).

La organización siempre debe tener el plan de contingencias en caso de que se necesite un centro de emergencia paralelo en donde se puedan restaurar la información y continuar con la operatividad de la empresa.

Si bien la empresa debe tener un plan para combatir las emergencias también es necesario que cuente con medidas de seguridad para evitar la sustracción de los equipos informáticos, el sistema de red y los periféricos. A continuación detallaremos un conjunto de medidas de seguridad física para las organizaciones:

Acceso de personas al recinto

Se debe tener un control de máxima seguridad para las personas que no están autorizadas al ingreso donde está localizado el hardware que utiliza la empresa, de tal forma que solo puedan utilizar los usuarios asignados para esa área, se puede hacer uso de tarjetas magnéticas para el personal para el acceso a una o varias zonas y también el uso de video vigilancia, seguridad personal y seguridad biométrica (huellas dactilares) y tener un control total de todas las instalaciones.

Alarma contra intrusos. Es importante para proteger el hardware y software de personas no autorizadas para que no puedan ingresar a áreas significativas y se las pueda detectar en caso de algún evento probable.

Un sistema de alarma puede contener los siguientes elementos:

- a) **Un módulo central.** Es una consola de seguridad electrónica que administra los componentes y los coordina, contiene la activación y desactivación por voz o por contraseña de los componentes que están a su cargo.
- b) **Detectores.** Pueden ser sensores que detectan variaciones de temperatura y volumen del espacio que abarcan, estos a su vez asociados con cámaras de seguridad que capturan las imágenes de posibles intrusos y los envía a la consola de seguridad.

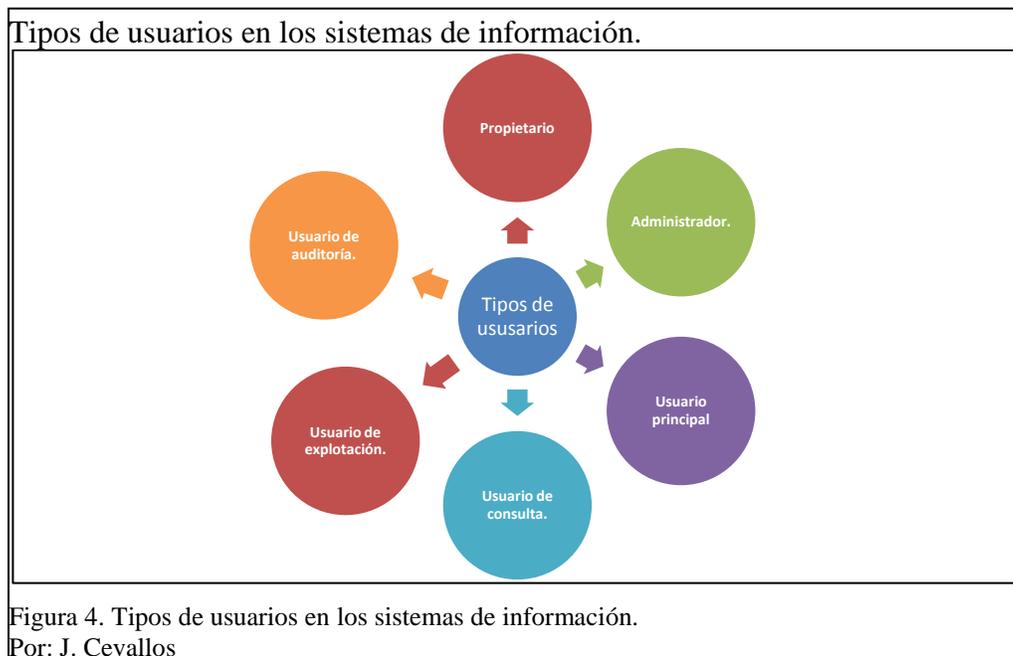
- c) **Sistema de cableado.** Interconexión de los sistemas de seguridad de forma inalámbrica.
- d) **Baterías autónomas o de emergencia.** En caso de interrupción de la energía deben de funcionar de la misma forma en todos los dispositivos.
- e) **Contactos magnéticos.** Se colocan generalmente en puertas y ventanas para que a ciertas horas no exista el acceso al personal sin autorización.
- f) **Avisador telefónico.** Son sistemas de alarma que a través de una llamada o un mensaje de texto informar sobre alguna actividad e informan al personal especializado.
- g) **Pulsadores de emergencia.** Son botones de emergencia que instalan en las oficinas en caso de existir posibles robos, activa la alarma y envía una señal de emergencia a la consola y el personal de seguridad.
- h) **La alarma.** Es el dispositivo físico que emite un sonido acústico que indica que existe un posible ataque a la seguridad.

1.7.2.2 Seguridad lógica. “Es toda aquella relacionada con la protección del software y de los sistemas operativos que en definitiva es la protección directa de toda la información y los datos”. (Aguilera López, 2010, pág. 30). Es la seguridad al software que contiene la información de las actividades de la organización, es indispensable que cada equipo (hardware) contenga las debidas seguridades de controles de accesos claves de seguridad y sea asignado a un usuario específico porque de esto depende la seguridad de los datos.

Cuando no existe seguridad lógica o existe una violación de la misma puede traer una serie de consecuencias graves y (Echenique García, 2004, pág. 195) en su libro detalla las siguientes:

- a) Cambio de datos antes o cuando se le da entrada en la computadora.
- b) Copias de programas y/o información.
- c) Código oculto o malicioso en algún programa.
- d) Entrada de virus.

Así tenemos los diferentes tipos de usuarios que pueden utilizar los sistemas de información de acuerdo a la información del libro de (Echenique García, 2004, pág. 196) así:



Propietario. Es el responsable y dueño de la información, puede consultar crear, modificar eliminar y dar autorizaciones a otros usuarios.

Administrador. Es el responsable de actualizar o modificar el software, no puede modificar la información se encarga de la seguridad lógica.

Usuario principal. Es el responsable de manejar la información puede modificarla y hacerle cambios.

Usuario de consulta. Solo puede leer la información.

Usuario de explotación. Autorizado para leer la información y emitir reportes de la misma.

Usuario de auditoría. Rastrea toda la información del sistema para detectar posibles fallos emite una opinión de aquello que necesita encontrar en el sistema y lo remite a la administración.

Existen algunas áreas que abarca la seguridad lógica están son:

Encriptación o cifrado. “Es el proceso mediante el cual se cifra la información o texto de tal forma que resulte ilegible, la única forma de interpretar la información es con la clave de seguridad”. (IWI, 2009, pág. 61). Por lo tanto a través de una clave de seguridad se encripta la información y solo a través de la misma se la puede volver a convertir en datos para su interpretación.

Los algoritmos de encriptación. Son los métodos de cifrado que se puede utilizar al momento de realizar encriptación de la información estos pueden ser de tres tipos como nos detalla: (Acissi, 2013, pág. 129) en su libro de la siguiente forma:

- a) Clave simétrica
- b) Clave asimétrica
- c) Hash

Clave simétrica. “Este algoritmo es el primero de todos utiliza la misma clave para cifrar y para descifrar se utilizó hasta principios de los años ochenta”. (Corletti Estrada, 2011, pág. 443).

Existen algunos tipos de claves simétricas que se usan estas son:

DES. “Es el estándar de cifrado de datos o Data Encryption Standard es el algoritmo simétrico mas utilizado del mundo desde 1977, fue utilizado para comunicaciones no clasificadas por el gobierno de los E.E.U.U”. (Maciá Perez, y otros, 2008, pág. 225)

IDEA. “Es un algoritmo suizo muy potente es muy rápido y puede usar claves de 128 bits es un algoritmo de alta seguridad”. (Acissi, 2013, pág. 129)

AES. “Es un sistema simétrico de cifrado por bloque diseñado para utilizar longitudes de clave y bloques variables de 128 y 256 bits está diseñado para resistir criptoanálisis lineal y diferencial”. (Maciá Perez, y otros, 2008, pág. 227).

BLOWFISH. “Es un cifrado de 64 bits reciente es un referente en el mundo de la criptografía es muy rápido y potente se usa en aplicaciones militares”. (Acissi, 2013, pág. 129)

RC5. “Este sistema es variable y configurable en todos sus aspectos puede utilizar diferente tamaños de bloque como 32, 64, 128 bits”. (Maciá Perez, y otros, 2008, pág. 227)

Clave asimétrica. Es una técnica se basa en el empleo de dos claves una publica la cual se difunde sin ninguna limitación y la privada la cual es conocida únicamente por el propietario en la actualidad resulta alta en costo pero también en beneficio porque resulta altamente confiable y segura en la actualidad.

Adicionalmente el autor antes mencionado describe tres problemáticos que se pueden usar en este cifrado estos son:

- a) Logaritmos enteros discretos
- b) Factorización de números.
- c) Curvas elípticas.

RSA. “Es el tipo más común de cifrado asimétrico es un criptosistema de clave pública que se basa en el hecho de que cuando más grande es el numero más tiempo dura la descomposición de los factores primos”. (Acissi, 2013, pág. 129)

Algoritmos Hash. “Es un método que se utiliza para firmar electrónicamente un mensaje basándose en que prácticamente imposible que dos mensajes puedan tener la misma firma digital, para asegurar la integridad del mensaje transmitido”. (Acissi, 2013, pág. 131)

Existen algunos tipos de algoritmos hash estos son los principales:

MD5. “Este algoritmo toma como entrada un mensaje de longitud arbitraria y produce como salida un resumen de mensaje de 128 bits”. (Stallings, 2004, pág. 67)

SHA-1. “Apareció en 1994 se considera libre y seguro produce un hash de 160 bits este algoritmo emplea 5 variables en lugar de 4 como usa el MD5 e inclusive es mayor el número de operaciones que realiza”. (Díaz, Mur, Sancristobal, Castro, & Peire, 2012, pág. 320)

Autenticación e identificación de usuarios (contraseñas). Es una de las primeras acciones que debe tener una empresa, proteger la información de acuerdo al usuario que necesite utilizar la información.

Antivirus. Detectan e impiden la entrada de virus o software malicioso al sistema informático, debe de tener la capacidad de prevenir, detectar y corregir toda la información.

Corta fuegos (firewall). Es un software informático conectado también al hardware que permite o restringe el acceso al sistema para proteger la información.

La biometría. “Es la aplicación de técnicas matemáticas y que también pueden ser estadísticas en base a los rasgos físicos o de comportamiento de una persona de tal forma que sea posible poder identificarlos”. (IWI, 2009, pág. 62). Es necesario tomar en cuenta estos elementos porque contemplan de gran manera la seguridad de la organización para que estén salvaguardados sus datos, así como también las instalaciones físicas y equipos de trabajo, siempre se deben tomar decisiones para mantener actualizadas las medidas de salvaguarda de software y hardware porque solo así se puede mantener en conjunto las operaciones y desarrollo de la organización en materia de prevención y control de la seguridad.

1.8 La toma de decisiones. “Toda decisión es un dictamen, una elección entre varias alternativas. Una decisión es una alternativa compuesta de dos cursos de acción que probablemente se hallen a la misma distancia de la verdad”. (Madrigal Torres, 2009, pág. 113). Es el proceso para elegir qué alternativas tomar, por medio de una decisión la misma que es evaluada conforme a nuestra capacidad y para la mejora constante de los procesos y operaciones, para esto, es necesario tomar en cuenta que estas decisiones afectan a todos los recursos de la organización, el material, el humano, el tecnológico es por eso que una decisión puede cambiar el curso de la organización, de ahí que los administradores deben tener la suficiente información, conocimiento y experiencia para enfrentar cada uno de los problemas con decisiones acertadas para el mejor desempeño de la misma en todos los ámbitos donde se desarrolla.

1.9 Importancia de la toma de decisiones. “Tanto en el ámbito personal como en el medio administrativo y directivo, todas las personas toman decisiones a cada momento, día a día, en cada fase de las etapas de un proyecto o un programa”. (Madrigal Torres, 2009, pág. 114). Todas las personas tomamos decisiones nos enfrentamos todos los días a problemas simples y complejos pero que se derivan en la elección de una alternativa sea buena o mala, desencadena en una acción que nos permite ver las consecuencias de esa elección, y esta a su vez nos da como resultado todo aquello que queremos conseguir o a la inversa nos permite ver en que fallamos, lo corregimos y de nuevo empieza el ciclo para escoger la mejor alternativa.

Toma de decisiones individual. Es el proceso durante el cual una persona debe escoger entre una o varias alternativas. En el proceso administrativo inicia en la primera etapa, que es la previsión. En el contexto laboral, el directivo es la persona clave en relación con la toma de decisiones. Es el que por lo regular toma las decisiones u orienta a que éstas se tomen. (Madrigal Torres, 2009, pág. 114)

Una decisión individual se le atribuye a todos los miembros de la organización porque de alguna manera tienen que tomar decisiones de su trabajo, pero también este concepto hace referencia a las decisiones del administrador o el director de la

compañía el mismo que sabe y conoce del entorno de la organización y en base a la información que tiene puede realizar juicios de valor o emitir una orden basado en alternativas que se le puedan presentar de acuerdo a su capacidad para la dirección.

Arboles de decisión. Un árbol de decisión es una representación gráfica del proceso de decisión que indica las alternativas de decisión, los estados de la naturaleza y sus respectivas probabilidades, y los resultados para cada combinación de alternativa de decisión y estado de la naturaleza. a (Haizer & Mender, 2008, pág. 314)

A través de un gráfico se definen cuáles son las alternativas de solución y de cada una de esas cuales es la que podemos elegir, una elegida la opción de ella se desprende múltiples soluciones por lo tanta se las debe analizar una por una y escoger la mejor.

1.10 Modelos de toma de decisiones

Los modelos de toma de decisiones son los tipos de decisiones que podemos tener en el momento que se presenta un problema o una situación, es necesario analizar cada una de ellas y su afectación que tienen al escogerlas para su posterior aplicación en la organización.

Tipos de entorno en la toma de decisiones. Existen tres tipos de decisiones comúnmente aceptadas al momento de hacer una selección de la mejor alternativa de esta forma tenemos tres tipos estos son:

- a) Toma de decisiones bajo incertidumbre
- b) Toma de decisiones con riesgo
- c) Toma de decisiones con certeza

1.10.1 Toma de decisiones bajo incertidumbre. “Cuando existen varios estados de la naturaleza y el administrador no puede evaluar con confianza la probabilidad del resultado o cuando prácticamente no existe dato alguno acerca de la probabilidad el ambiente se llama toma de decisiones bajo incertidumbre”. (Render, Hanna, & Stair,

2006, pág. 71). En este caso no tiene todos los datos, o en definitiva no tiene los datos concretos entonces se tiene que tomar decisiones bajo incertidumbre pero bajo las siguientes condiciones:

- a) Maximax (optimista)
- b) Maximin (pesimista)
- c) Criterio de realismo (Hurwicz)
- d) Igualdad de probabilidades de (Laplace)
- e) Arrepentimiento minimax.

Para nuestro estudio únicamente estudiaremos los tres más importantes que son el maximax, maximin, y el de igualdad de probabilidades.

Maximax. Este método selecciona la alternativa que maximiza el resultado máximo de cada una de las alternativas. En primer lugar, se halla el máximo resultado de cada alternativa, y después se elige la alternativa con el valor máximo. Como este criterio de decisión localiza la alternativa con la mayor posible ganancia, ha sido denominado criterio de decisión “optimista”. (Haizer & Mender, 2008, pág. 310).

En base al concepto anterior afirmamos que de las mejores alternativas de solución que se puedan dar, escogemos la opción con la alternativa que genere mayores resultados en su conjunto con las demás alternativas, este criterio se le denomina optimista porque ya se tienen opciones positivas para tomar una decisión pero de todas estas buscamos la que se adapte y beneficie en su conjunto y sea la mas adecuada para la organización.

Maximin. Este método selecciona la alternativa que maximiza el resultado mínimo de cada una de las alternativas. En primer lugar, se halla el resultado mínimo de cada alternativa, y después se escoge la alternativa con el valor máximo. Dado que este criterio de decisión localiza la alternativa que tiene la menor pérdida posible, se lo ha

denominado criterio de decisión pesimista. (Haizer & Mender, 2008, pág. 310)

El método maximin escoge la alternativa con el valor mínimo una vez realizado esto de todas las alternativas que aparezcan se tomará la más alta con el valor mínimo este proceso no es muy convincente ni tampoco conveniente ya que trata de maximizar una alternativa que se encuentra por debajo del máximo por lo tanto al escoger esta opción se trata de obtener la menor pérdida posible, entonces se trata de una idea de no forzar mucho los recursos de la organización y no tomar riesgos en este caso solo se trabaja a la segura con este método.

Igualdad de probabilidades. “Este enfoque involucra encontrar la ganancia promedio de cada alternativa y seleccionar aquella que ofrezca el promedio más alto”. (Render, Hanna, & Stair, 2006, pág. 74). Este método concibe la idea de que cada alternativa se determine una ganancia promedio y después se pueda seleccionar la ganancia con mayor promedio, por lo tanto puede ocurrir que una alternativa bajo determinadas condiciones que presente mayor valor promedio, ejemplo en un época del año alta una alternativa puede ser mejor que otra, pero la misma alternativa en otro período de tiempo puede resultar con menor valor promedio y depende de la naturaleza de la alternativa para su elección.

1.10.2 Toma de decisiones con riesgo

Es una situación en la cual podrían presentarse varios posibles estados de la naturaleza, y se conocen las probabilidades de todos ellos, por lo tanto la selección de la alternativa con el valor monetario esperado más alto (o simplemente el valor esperado), también se utiliza las probabilidades con la tabla de pérdida de oportunidades a fin de minimizar la pérdida de oportunidad esperada. (Render, Hanna, & Stair, 2006, pág. 75).

En este tipo de toma de decisiones se presentan varios posibles opciones, por ejemplo, un mercado favorable o un mercado desfavorable, en el que podemos

invertir y tenemos un porcentaje de ingreso o un valor esperado, o tenemos la otra opción que es el no invertir no hacer nada y obtener un valor esperado, es necesario conocer el ambiente donde se va a tomar decisiones los cambios sociales, económicos, políticos y como estos pueden afectar a futuro nuestras decisiones ya sean favorables o desfavorables siendo este el caso más extremo.

Valor monetario esperado. Esta cifra representa el valor esperado o rendimiento medio de cada alternativa, si pudiéramos repetir la decisión en un gran número de veces. El EMV (Expected monetary value) para una alternativa es la suma de los posibles resultados de la alternativa, cada uno de ellos ponderado por la probabilidad de que ocurra. (Haizer & Mender, 2008, pág. 312)

El valor monetario esperado es simplemente la suma de los posibles pagos que esta alternativa ofrece y cada debe estar ponderado por la probabilidad de que el pago ocurra.

Ejemplo: Tomado del libro Métodos cuantitativos para la toma de decisiones.

Suponga que ahora John Thompson cree que la probabilidad de un mercado favorable es exactamente la misma que la probabilidad de un mercado desfavorable, es decir, cada estado de la naturaleza tiene una probabilidad de 0,50 ¿Cuál alternativa daría mayor monetario esperado? Para dilucidar esta cuestión, John ha expandido su tabla de decisión, y sus cálculos son los siguientes.

$$\text{EMV (fabrica grande)} = (0,50) (\$200.000) + (0,50) (-\$180.000) = \$ 10.000$$

$$\text{EMV (fabrica pequeña)} = (0,50) (\$100.000) + (0,50) (-\$20.000) = \$ 40.000$$

$$\text{EMV (hacer nada)} = (0,50) (\$0) + (0,50) (\$0) = \$0$$

El valor esperado más grande es (\$40.000) es el que ofrece la segunda alternativa, construir una fábrica pequeña, con base a ello, Thompson debería llevar a cabo el proyecto y abrir una pequeña fábrica para producir los cobertizos de almacenamiento. Los valores del EMV de una fábrica grande y de hacer nada son de \$10.000 y \$0 respectivamente. (Render, Hanna, & Stair, 2006, pág. 76).

Analizando este ejemplo determinando el valor esperado en este caso los \$ 40.000 son la opción correcta ya que tomando en cuenta el mercado favorable y el desfavorable al abrir una fábrica pequeña nos da mayor valor monetario esperado para la empresa, entonces supera ampliamente a la opción de abrir una fábrica grande y al hecho de no hacer nada.

1.10.3 Toma de decisiones con certeza. “La toma de decisiones bajo certidumbre, quienes la conocen con certeza la consecuencia de cada una de las alternativas, naturalmente seleccionará la opción que maximizará su bienestar o que dará mejor resultado”. (Render, Hanna, & Stair, 2006, pág. 70). Al analizar este tipo de decisiones se puede deducir que la persona que toma estas decisiones puede predecir con certeza las consecuencias de cada alternativa de acción y sabe que hacer en un mercado favorable y también en un mercado desfavorable, de ahí que la capacidad de los administradores, directores y gerentes para ampliar el mejor manejo de los recursos y maximizar los resultados.

1.11 Evaluación y selección de las alternativas para la decisión final

En la evaluación y selección se identifican los puntos clave que deben de tener en consideración los administradores o los directivos de la organización para evaluar las alternativas y escoger cuales son las factibles para la empresa y como estas influyen en la decisión final.

Cuando se eligen las alternativas en primera instancia son evaluadas, pero como se hace esto, dependiendo de la organización se deben medir en términos de resultados, si son rentables si generan utilidad todo esto haciendo simulaciones, también tenemos

que tomar en cuenta los riesgos que pueden ocasionar las alternativas por ejemplo el costo beneficio, el margen de rentabilidad y si a futuro en el transcurso del plan de acción se pueden mitigar los riesgos a los que se puedan enfrentar, y por último se debe también hacer una evaluación de los recursos de la empresa ya que si los recursos no se encuentran disponibles, entonces las posibles soluciones no tendrán un respaldo para su iniciación de tal forma que es mejor analizar los elementos disponibles en la empresa como son los recursos materiales, los financieros, los humanos versus los costes, las ventajas y las desventajas que se pueden obtener a través de la decisión.

Después de haber encontrado las soluciones pues debemos implantarlos así: “Una solución bien elegida no siempre tiene éxito. Una decisión técnicamente correcta debe ser aceptada y apoyada por las personas que se encargarán de su implementación para que haya una actuación efectiva basada en la decisión”. (Hellriegel, Jackson, & Slocum, 2009, pág. 270). En base a lo expuesto anteriormente se necesitan de todos los recursos en torno a la decisión tomada para que la misma surta efecto y depende en buena parte de las personas que están a cargo de la implementación para que aparezcan resultados positivos.

En la evaluación los directores y los administradores eficaces buscan la forma adecuada para: “Minimizar las desventajas de la opción seleccionada y maximizar sus ventajas y beneficios”. (Santos, 2007, pág. 222). En este párrafo se refiere que los resultados que se esperan alcanzar cumplan con los objetivos determinados por la organización y que fueron establecidos para un fin en especial.

A continuación después de toda decisión se debe de tener un plan de acción no es más que asignar tareas, definir el tiempo y los plazos en los que se va a realizar, y también el uso de los recursos que se van a utilizar, por ultimo existe la evaluación del plan de acción es decir hacer pruebas y detectar problemas que se puedan suscitar de tal forma que puedan tomar acciones alternativas que permitan superar divergencias en la implantación.

Después de tener el plan de acción listo se lo debe implantar y en conjunto con la decisión se debe dar un seguimiento adecuado que permita controlarlo y verificar si se están cumpliendo todas las tareas asignadas para el cumplimiento de los objetivos.

La implantación de la solución que se ha preferido no logrará de forma automática la meta deseada. Las personas o los equipos deben controlar las actividades de implementación y después darle seguimiento evaluando los resultados de la misma. Si la implementación no está produciendo resultados satisfactorios será necesario aplicar medidas correctivas. (Hellriegel, Jackson, & Slocum, 2009, pág. 270)

En este caso siempre es necesario controlar habitualmente todos los procedimientos asignados al plan de acción y la decisión escogida siempre debe estar en constante análisis verificando su avance en el transcurso de las operaciones, la retroalimentación también es importante ya que permite analizar los resultados y nos da una idea de lo qué se desea cambiar qué se puede modificar y qué se puede eliminar, así como también si no está generando buenos resultados, por lo tanto iniciar un nuevo proceso de toma de decisiones y cambiar las alternativas de solución al problema.

CAPÍTULO 2

LAS FIRMAS DE AUDITORÍA DEL CANTÓN QUITO

2.1 Antecedentes

Para iniciar con el análisis de las firmas auditoras debemos entender a la auditoría, su enfoque inicial, como se inició el estudio llevado de la mano del control interno y cómo ha evolucionado a nuestra época actual. “De las diversas formas como se puede estudiar la evolución del control interno aquí se emplea una derivada del análisis y evolución de la auditoría a partir de esquemas de revisión (edad media 1880s), atestación (1880s -1990s) y aseguramiento (1990s-hoy)”. (Mantilla & Cante S., Auditoría de Control Interno, 2005, pág. 25)

Tabla 3.
Historia de la auditoría.

 Historia de la auditoría - Un enfoque conceptual			
	Edad Media i-business	Industrial L- business	Informática e-business
Componente Principal	Inventarios	Legalidad (Estatad, profesional o técnica)	Electrónica (Tecnología de la información)
Énfasis Organizacional	Patrimonio	Jerarquías	Proceso (Cadena de Valor)
Materia Prima	Datos	Información (Estados Financieros)	Conocimiento (Presentación de reportes sobre valor)
Definición	REVISORIA Comprobación y verificación al 100% de inventarios (Mercancías, efectivo, títulos valor, etc.)	AUDITORÍA INDEPENDIENTE Análisis, pruebas (estadístico y no estadístico)	ASEGURAMIENTO Evaluación de riesgos de negocio (Entono, clientes, mercados, competencia, etc.)
Criterio	Lo que diga el inventario	Lo que diga la norma	Lo que aporte al negocio. Generación de Valor

Fuente: Tomado parcialmente de Auditoría 2005

Nota: Enfoque conceptual de la historia de la auditoría.

Para diferenciar cada una de estas etapas en las que se puede observar en la Tabla 3, se describirán cada una de ellas de acuerdo a su aparición y momento en el tiempo.

En los inicios la primera generación se basa en acciones empíricas, a partir de procedimientos de ensayo error, la principal causa de su insistente aplicación se debe en buena parte a una carencia de profesionalización de quienes tienen a su cargo el sistema de control interno. En la primera etapa la aparición de la auditoría se basaba más a manera de pruebas ya que en su inicio era muy tedioso realizar el trabajo por la complejidad y la falta de sistemas informáticos y tecnología que ayude a facilitar el trabajo.

En la segunda generación se encuentra marcada por marco legal, se logran imponer estructuras y prácticas de control interno especialmente en el sector público, pero desafortunadamente se dio una conciencia distorsionada de este al hacerlo operar muy cerca de la línea de cumplimiento formal y lejos de los niveles de calidad técnicos que requerían en esos momentos la práctica de una auditoría confiable para los usuarios. (Mantilla & Cante S., Auditoría de Control Interno, 2005).

En esta fase de la auditoría con la ayuda de la parte legal se lograron enfocar sus esfuerzos para lograr controles de calidad en las organizaciones, pero se centra más en el cumplimiento que en la eficiencia de las operaciones porque estaban más preocupados por los organismos de control y de tener al día y en orden los papeles pero no se concentraba en la toma de decisiones por parte de la gerencia lo cual implicaba una excesiva pérdida de recursos ya que todos los recursos se enfocaban más al cumplimiento.

La tercera generación es la actual la cual centra sus esfuerzos en la calidad derivada del posicionamiento en los más altos niveles estratégicos y directivos, como requisito mínimo que garantiza la eficiencia del control interno, es aquí donde se reconoce el fruto de los esfuerzos originados por COSO (Committee of Sponsoring Organizations of the Treadway Commission) hacia los años 90s, los cuales han sido estructurados y completados de acuerdo a los nuevos direccionamientos estratégicos, el ascenso en la escala organizacional y reforzados por los alcances de la Sarbanes-Oxley Act de 2002

(Ley para el mercado de Valores de los Estados Unidos y respuesta a la crisis de Enron y relacionados). (Mantilla & Cante S., Auditoría de Control Interno, 2005)

En esta última generación se centra más en la eficacia y en la eficiencia de las operaciones además del cumplimiento que deben tener para con los organismos reguladores, se incorpora el informe COSO el cual trataba de mejorar e incrementar el control interno en todas las operaciones del ciclo contable, todo esto en función de los objetivos planteados por la organización y delimitados en la planeación de aquí que la importancia de la auditoría para evitar los fraudes, controlar los recursos utilizados y tomar decisiones que generen un incremento en la capacidad productiva en la organización, el marketing, ventas y a dónde desea llegar a futuro.

2.2 La auditoría

Para iniciar con el estudio de la auditoría definiremos el concepto de auditoría para su mejor comprensión así:

Auditoría es el examen integral sobre la estructura, las transacciones y el desempeño de una entidad económica, para contribuir a la oportuna prevención de riesgos, la productividad en la utilización de los recursos y el acatamiento permanente de los mecanismos de control implantados por la administración. (Sanchez Guriel, 2006, pág. 2)

La auditoría se encarga de la verificación de las operaciones de la entidad, para emitir una opinión de si se presentan de acuerdo a la normativa vigente y como se pueden mejorar e incrementar el control interno de la organización a través de optimización de recursos y de esta manera contribuir a los administradores para que tomen decisiones oportunas basadas en información confiable.

Existen además algunas definiciones de auditoría de acuerdo a su campo de estudio las mismas que detalla a continuación:

Auditoría de estados financieros. Es el examen y verificación de los estados financieros de una empresa con el objeto de emitir una opinión sobre la fiabilidad de los mismos.

Esta definición se basa en la verificación a los estados financieros de si se presentan razonablemente de acuerdo a las normas y procedimientos vigentes y en base a esta información emitir una opinión.

Auditoría de informes económicos y financieros. Aparte de las cuentas anuales cualquier información económica puede ser sometida a examen o verificación con el objeto de opinar sobre su veracidad, transparencia y razonabilidad de cálculo.

En esta definición nos referimos a la auditoría de los informes finales que permiten tomar decisiones y lo que se trata de verificar es que todas aquellas decisiones que fueron tomadas por la organización se basaron en información confiable y segura.

Auditoría interna. Tiene por objeto verificar los diferentes procedimientos y sistemas de control interno establecidos en una empresa.

A través de la auditoría interna se trata de verificar los procedimientos de control interno que realiza la empresa con el fin de mantener una medición adecuada de aquellos procesos que la empresa utiliza para el giro de su negocio.

Auditoría operativa. El objetivo es el examen de la gestión de la empresa con el propósito de evaluar la eficacia de los resultados con respecto a las metas previstas.

En esta definición nos referimos a la evaluación de las decisiones tomadas por la dirección con respecto a cumplir los objetivos propuestos por la organización de tal forma que se puedan identificar aquellos problemas que no permiten el desarrollo organizacional y productivo de la entidad.

Auditoría de sistemas. La finalidad es el examen y análisis de los procedimientos administrativos y de los sistemas de control interno de la compañía auditada para establecer: la eficacia de los procedimientos establecidos, la idoneidad de los criterios contables, la funcionalidad de sus circuitos y sistemas administrativos.

En la auditoría se busca verificar los controles sobre el procesamiento de la información, la evaluación de los procesos que se realizan de forma automática para el tratamiento de los datos y como todos los recursos informáticos se relacionan entre sí para validar toda la información obtenida.

Auditoría económico-social. Este concepto está vinculado con la necesidad de evaluar la aportación que la empresa hace al progreso humano, o dicho de otra forma contribuir al cumplimiento de la responsabilidad social.

En este tipo de auditoría nos referimos al aporte que realiza la organización al desarrollo de la sociedad, es decir, como contribuye para el desarrollo común a través de proyectos inversión y de inserción social que aporten al mejoramiento de la calidad de vida, de aquí la importancia de que se cumplan estos proyectos median controles y evaluación a dichos proyectos.

2.3 Tipos y técnicas de auditoría

A continuación se detalla la clasificación de la auditoría de la siguiente forma:

Auditorías por su lugar de aplicación. En este tipo de auditorías permiten verificar procesos y procedimientos internos de una organización y cuando se analiza fuera de la misma queremos obtener el grado confiabilidad de la gestión que se realiza.

- a) Auditoría Interna
- b) Auditoría Externa

Auditorías por su área de aplicación. Se las realiza de acuerdo a un ámbito específico de un área de trabajo, rama o especialidad que va a ser motivo de revisión y evaluación.

- a) Auditoría financiera,
- b) Auditoría administrativa,
- c) Auditoría operacional,
- d) Auditoría integral,
- e) Auditoría gubernamental
- f) Auditoría sistemas.

Auditorías especializadas en áreas específicas. Este tipo de auditorías están enfocadas a satisfacer necesidades específicas de revisión de una organización.

- a) Auditoría al área médica (evaluación médico-sanitaria),
- b) Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería),
- c) Auditoría fiscal
- d) Auditoría laboral
- e) Auditoría de proyectos de inversión, a la caja chica o caja mayor (arqueos), al manejo de mercancías (inventarios)
- f) Auditoría ambiental

Auditoría de sistemas computacionales. Este tipo de auditorías se basa en la revisión exhaustiva del hardware y software que utiliza la empresa con el fin optimizar sus recursos al realizar sus operaciones informáticas.

- a) Auditoría informática, con la computadora, sin la computadora,
- b) Auditoría a la gestión informática
- c) Auditoría al sistema de cómputo, alrededor de la computadora, de la seguridad de sistemas computacionales, a los sistemas de redes, integral a los centros de cómputo, ISO-9000 a los sistemas computacionales, outsourcing y ergonómica de sistemas computacionales.

2.3.1 Requerimientos mínimos de competencias de un auditor informático

El auditor informático debe tener cierto tipo de competencias y conocimientos que le permitan obtener de manera confiable la información y se las detalla así:

- a) El auditor informático debe tener buena preparación, tanto teórica como práctica de tal forma que pueda tomar decisión sobre la información revisada y evaluada.
- b) La cualificación del auditor la misma que debe ser educación y experiencia, debe tener habilidad de comunicación, entrenamiento en sistemas de información y participación en auditorías de sistemas de información.
- c) También se pueden detallar algunas características como: recomendar, ser independientes, y objetivos tener el conocimiento sobre sistemas de información, diagnosticar los datos que se analizan en función de las verificaciones y mantenerse siempre actualizado. (De Pablos Carmen, 2011, pág. 335)

2.3.2 Técnicas de auditoría

Las técnicas de auditoría son los métodos que utiliza el auditor para obtener evidencia que le permite emitir su opinión y las detalla (Cardozo Cuenca, 2006, pág. 18) en su libro así:

- a) Estudio general
- b) Análisis
- c) Inspección
- d) Confirmación
- e) Investigación
- f) Declaraciones o certificaciones

- g) Certificación
- h) Observación
- i) Cálculo.

Estudio general. “Es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones, a través de sus elementos más significativos para elaborar las conclusiones se ha de profundizar en su estudio y en la forma que ha de hacerse”. (Cardozo Cuenca, 2006, pág. 18). En este punto se hace un estudio en general de toda la situación de la empresa y las operaciones para poder planificar y realizar el plan de auditoría para poder ver si es factible o no la auditoría.

Análisis. “Es el estudio de los componentes de un todo. Esta técnica se aplica concretamente al estudio de las cuentas o rubros genéricos de los estados financieros”. (Cardozo Cuenca, 2006, pág. 18). En esta etapa se analizan las cuentas de si están presentadas de acuerdo a las normas vigentes, y se lo realiza una por una para encontrar diferencias o si existe error intencional o no.

Inspección. “Examen físico de los bienes materiales o de los documentos, con el objeto de cerciorarse de la existencia de un activo o de una operación registrada o presentada en los estados financieros”. (Luna, 2003, pág. 155). Verificación de las existencias de activos inventarios y documentos de la empresa para su respaldo en el ciclo contable.

Confirmación. “Obtención de una comunicación escrita de una persona independiente de la empresa examinada y que se encuentre en posibilidad de conocer la naturaleza y condiciones de la operación y por lo tanto, confirmar de una manera valida”. (Luna, 2003, pág. 156). Esta es una confirmación que se realiza por lo general a las entidades financieras con el fin de verificar saldos, créditos, inversiones de tal forma que esta información se valide con las cuentas de los estados financieros.

Investigación. “Es la recopilación de información mediante entrevistas o conversaciones con los funcionarios y empleados de la empresa”. (Cardozo Cuenca,

2006, pág. 19). Es la recopilación de la información que se realiza en la organización a fin de tener una certeza razonable de las operaciones, el control interno, la administración, y el manejo de los recursos, a través de la indagación y encontrar posibles divergencias.

Declaraciones o certificaciones. “Es la formalización de la técnica anterior, cuando, por su importancia resulta inconveniente que las afirmaciones recibidas deban quedar escritas (declaraciones) y en algunas ocasiones certificadas por una autoridad (certificaciones)”. (Cardozo Cuenca, 2006, pág. 19). En este punto se tiene un documento válido que certifica que la información obtenida la obtuvieron de manera legal, por ejemplo a través de una entrevista, una encuesta, una prueba y se obtiene el respaldo de quién y en qué momento lo realizó.

Certificación. “Obtención de un documento en el que se asegure la verdad de un hecho, legalizado por lo general, con la firma de una autoridad”. (Luna, 2003, pág. 157). Es decir en este punto se obtiene una certificación firmada por el responsable de manejar la información que se solicita.

Observación. Es una manera de inspección, menos formal, y se aplica generalmente a operaciones para verificar como se realiza en la práctica, esta técnica permite observar de manera general un proceso, una actividad, una tarea de tal forma que se tiene una idea de cómo se realiza estas operaciones en las organizaciones.

Cálculo. “Verificación matemática de alguna partida o de alguna operación”. (Luna, 2003, pág. 157). Es la comprobación que se realiza matemáticamente a toda la información presente en los estados financieros o en las actividades que demanden y arrojen valores numéricos de tal forma que se puedan comprobar los resultados.

2.4 Objetivos de la auditoría

De manera general una auditoría se refiere a un conjunto de objetivos que se deben cumplir y que se refieren a la capacidad del auditor para encontrar todos aquellos

sucesos que pueden resultar en problemas para la empresa, los objetivos que se muestran a continuación son una base a considerar en el desarrollo de una auditoría:

- a) Mitigar y prevenir las irregularidades y el fraude comprobando la existencia de la diferencias en los registros contables.
- b) Comprobar que la organización cumple con las disposiciones legales vigentes.
- c) Comprobar si existe sistemas adecuados para el control y la dirección del negocio y así introducir las mejoras que se puedan integrar al negocio.
- d) Asegurar que los principios de contabilidad generalmente aceptados se presenten y se aplican de manera uniforme.
- e) Garantizar la presentación de los estados contables de tal forma que sirvan como un instrumento de toma de decisiones para los inversionistas, acreedores, accionistas y demás figuras públicas o privadas relacionadas con la institución.

A continuación vamos a describir el objetivo de la auditoría emitido por la IAASB (International Auditing and Assurance Standards Board) Consejo de Normas Internacionales de Auditoría y Aseguramiento, en la que se detalla así:

El objetivo de una auditoría es aumentar el grado de confianza de los usuarios en los estados financieros. Esto se logra mediante la expresión, por parte del auditor, de una opinión sobre si los estados financieros han sido preparados, en todos los aspectos materiales, de conformidad con un marco de información financiera aplicable. En la mayoría de los marcos de información con fines generales, dicha opinión se refiere a si los estados financieros expresan la imagen fiel o se presentan fielmente, en todos los aspectos materiales, de conformidad con el marco. Una auditoría realizada de conformidad con las NIA y con los requerimientos de ética aplicables permite al auditor formarse dicha opinión. (IAASB, 2009, pág. 57)

La opinión de los estados financieros tiene que basarse de acuerdo a la información financiera aplicable, pero esta opinión no afirma la eficacia o eficiencia de las

operaciones de una entidad a futuro, pero el auditor debe basarse en las NIA y si necesita realizar un trabajo suplementario para que la opinión de la información sea más confiable pues deberá hacerlo y asegurar su informe.

2.4.1 Objetivos globales del auditor

En la realización de la auditoría de estados financieros, los objetivos globales del auditor son:

La obtención de una seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material, debida a fraude o error, que permita al auditor expresar una opinión sobre si los estados financieros están preparados, en todos los aspectos materiales, de conformidad con un marco de información financiera aplicable. (IAASB, 2009, pág. 58)

La emisión de un informe sobre los estados financieros, y el cumplimiento de los requerimientos de comunicación contenidos en las NIA, a la luz de los hallazgos del auditor. (IAASB, 2009, pág. 58)

En esta parte afirmamos que la opinión del auditor debe basar en información confiable pero siguiendo las normas de información financiera y que además debe presentar un informe de auditoría con la opinión de tal forma que estén ligados al mejoramiento del control interno de la organización.

2.5 Las NIIF y las NIA

Las NIIF son las normas internacionales de información financiera por sus siglas en ingles (IFRS) International Financial Reporting Standard y se utilizan como:

Los estándares de la contabilización que la mayoría de los países latinoamericanos utilizan para el registro para el registro, valuación, presentación y revelación de las transacciones económicas que afectan

los estados financieros de todas y cada una de las entidades domiciliadas en esta zona geográfica. (Mesén Figueroa, 2007, pág. 11)

Estas normas son estándares que utilizan la mayoría de países del mundo y de Latinoamérica para todas sus transacciones económicas con el fin de unificar conceptos y definiciones con respecto al tratamiento de la información económica financiera para que la misma sea presentada de manera razonable.

Continuando con el estudio de las NIIF vamos a describir a la brevedad las normas internaciones de información financiera a través de una publicación de la empresa (Deloitte Touche Tohmatsu Limited, 2013) y que se describen así:

NIIF (IFRS)1. Adopción por primera vez de las Normas Internacionales de Información Financiera. Describe los procedimientos cuando la entidad adopta por primera vez las NIIF, y esta se convierte en la base para la preparación de los estados financieros.

NIIF (IFRS)2. Pagos basados en acciones. Describe la contabilidad a utilizar de una entidad adquiere o recibe bienes o servicios, ya sea que estos se incluyan en el patrimonio o conformen los pasivos en cantidades que se basan en el precio por acciones.

NIIF (IFRS)3. Combinación de negocios. La entidad que adquiere un negocio debe reconocer los activos adquiridos y los pasivos asumidos a sus valores razonables para evaluar su naturaleza y los efectos de la adquisición.

NIIF (IFRS)4. Contratos de seguro. Prescribe la información financiera para los contratos de seguro.

NIIF (IFRS)5. Activos no-corrientes mantenidos para la venta y operaciones descontinuadas. Describir la operación contable para los activos no-corrientes que se tienen para la venta y la presentación y revelación de las operaciones descontinuadas.

NIIF (IFRS)6. Exploración y evaluación de recursos minerales. Prescribir la información financiera sobre la explotación y evaluación de los recursos naturales.

NIIF (IFRS)7. Instrumentos financieros. Revelaciones. Prescribir las revelaciones que les permiten a los usuarios del estado financiero evaluar la importancia que los instrumentos financieros tienen para la entidad.

NIIF (IFRS)8. Segmentos de operación. La entidad tiene la obligación de revelar la información que permita a usuarios de los estados financieros evaluar la naturaleza y efectos de las actividades del negocio en las que participa.

NIIF (IFRS)9. Instrumentos financieros. Establece requerimientos de reconocimiento des-reconocimiento clasificación y medición para los activos y pasivos financieros.

NIIF (IFRS) 10. Estados financieros consolidados. Introducir un modelo único de consolidación para todas las entidades y que se basa en un control independiente de la naturaleza de la entidad donde se invierte.

NIIF (IFRS) 11. Acuerdos conjuntos. Elimina la opción de aplicar el método de consolidación proporcional cuando se contabilicen entidades controladas, elimina activos controlados y solo existe la diferenciación entre operaciones conjuntas y negocios conjuntos.

NIIF (IFRS) 12. Revelación de intereses en otras sociedades. Permite a los usuarios de los estados financieros evaluar la naturaleza de los riesgos asociados con intereses que entidad tiene con otras entidades y también los efectos de esos intereses en la posición financiera flujo y desempeño del efectivo.

NIIF (IFRS) 13. Medición del valor razonable. Establecer una definición del valor razonable, determinar y prescribir las revelaciones requeridas acerca de la medición del valor razonable.

Por otra parte las normas internacionales de contabilidad vigentes y que para nuestro estudio las detallaremos en base a la publicación de (Deloitte Touche Tohmatsu Limited, 2013) y que las describe así:

NIC 1. Presentación de estados financieros. Establece la estructura para la presentación de los estados financieros incluyen también las guías para su estructura y el contenido, los 5 estados son: estado de posición financiera, estados de resultados, estado de cambios en el patrimonio, estado de flujos de efectivo y las notas.

NIC 2. Inventarios Prescribir el tratamiento contable para los inventarios, debe incluir como se determina del costo y el reconocimiento de los gastos.

NIC 7. Flujos de efectivo Establece la presentación de información acerca de los cambios históricos acerca del efectivo y los equivalentes de efectivo de la entidad.

NIC 8. Políticas contables, cambios en las estimaciones contables y errores. Prescribe el criterio para la selección y cambio de las políticas de contabilidad, tratamiento contable y la revelación de los cambios en las políticas de contabilidad, los cambios en las estimaciones y los errores.

NIC 10. Eventos ocurridos con posterioridad al período sobre el que se informa. Cuándo la entidad debe ajustar sus estados financieros por los eventos ocurridos después del final del período de presentación de reporte.

NIC 11. Contratos de construcción. Prescribir el tratamiento contable en base a los ingresos ordinarios y costos asociados con contratos de construcción en los estados financieros del contratista.

NIC 12. Impuesto a las ganancias. Establecer los principios de contabilidad para el pago impuestos para recuperación de activos pasivos reconocidos en el estado de posición financiera además de los eventos que se produzcan en el período.

NIC 16. Propiedad, planta y equipo. Prescribe los principios para reconocer de forma inicial y también la contabilidad aplicada a la propiedad, planta y equipo.

NIC 17. Contratos de arrendamiento. Prescribe para los arrendatarios y los arrendadores, las políticas contables y revelaciones que sean adecuadas para los arrendamientos operacionales y financieros.

NIC 18. Ingresos ordinarios. Prescribe todo el tratamiento contable para los ingresos ordinarios por ventas de bienes, prestación de servicios, intereses, regalías y dividendos.

NIC 19. Beneficios a los empleados. Prescribe el tratamiento contable y la revelación de los beneficios a corto y largo plazo de los empleados.

NIC 20. Contabilización de las subvenciones del gobierno e información a revelar sobre ayudas gubernamentales. Prescribe el tratamiento contable y la revelación de las subvenciones del gobierno y otra forma de ayuda que puede brindar el gobierno.

NIC 21. Efectos en las variaciones en las tasas de cambio de la moneda extranjera. Prescribe la contabilidad para transacciones que la entidad realice en moneda extranjera y para operaciones en el exterior.

NIC 23. Costos por préstamos. Prescribe la contabilidad para los costos por préstamos, ya sean atribuibles a la adquisición, para construcción o la producción de un activo, todos los demás costos por préstamos se llevan al gasto cuando no se incurra en capitalización.

NIC 24. Partes relacionadas. Asegurar la posición de los estados financieros y los resultados aun cuando exista la posibilidad de ser afectados por partes relacionadas.

NIC 26. Contabilización e información financiera sobre planes de beneficio por retiro. Especifica la medición y la revelación que debe existir en los reportes financieros por planes de beneficio de retiro.

NIC 27. Estados financieros independientes (separados). Prescribe como se debe realizar el tratamiento contable de las inversiones que existen en subsidiarias, negocios conjuntos y asociadas en los estados financieros separados.

NIC 28. Inversiones en asociadas y negocios conjuntos. Establece la influencia de las inversiones en asociadas y prescribe el tratamiento contable del inversionista para inversiones en asociadas y negocios conjuntos.

NIC 29. Información financiera en economías hiperinflacionarias. Proporciona orientación específica para las organizaciones que reportan en moneda en una economía hiperinflacionaria, es decir cuando la tasa acumulada de inflación en 3 años se aproxima o se excede del 100%.

NIC 32. Instrumentos financieros: presentación. Prescribe los principios para clasificar los instrumentos financieros como pasivos o patrimonio y también para la compensación de activos y pasivos financieros.

NIC 33. Ganancia por acción. Determinar los principios para presentar las cantidades generadas por ganancias por acciones (GPA), con el fin de mejorar las comparaciones entre entidades de un mismo periodo.

NIC 34. Estados financieros intermedios. Determina el contenido mínimo que debe tener un reporte intermedio así como los principios de reconocimiento y medición.

NIC 36. Deterioro de valor. Asegurar los activos y verificar si son llevados a nomas de su cantidad recuperable y describir el cálculo de la cantidad recuperable, la pérdida por deterioro o su reversa.

NIC 37. Provisiones, pasivos contingentes y activos contingentes. Asegurar el cumplimiento de las normas para reconocer los activos y pasivos contingentes así como también en las notas a los estados financieros proporcionar información suficiente para que los usuarios reconozcan su naturaleza, oportunidad y cantidad.

NIC 38. Activos Intangibles. Determinar la contabilidad para el reconocimiento, medición y la revelación de todos los activos intangibles de manera específica.

NIC 39. Instrumentos financieros: Reconocimiento y medición. Establece los principios para el reconocimiento des-reconocimiento y medición de los activos y pasivos financieros

NIC 40. Propiedades de inversión. Prescribe la contabilidad para las propiedades de inversión y las revelaciones relacionadas.

NIC 41. Agricultura. Prescribe el tratamiento contable para la actividad agrícola, la administración y transformación de activos biológicos en productos agrícolas.

Las NIA son las normas internacionales de auditoría obligatorias para los auditores en un examen a los estados financieros y comprenden un conjunto de normas y de procedimientos para su realización. A continuación (Andrade Espinoza, 2012) detalla las NIA en su publicación así:

NIA 1 Objetivos y principios básicos de auditoría. El objetivo de la auditoría para los estados financieros deben ser preparados de conformidad con principios y prácticas contables vigentes de tal forma que el auditor exprese su opinión sobre dichos estados financieros.

NIA 2 Carta compromiso de auditoría. Es el documento que sustenta y confirma la aceptación del auditor, para la realización de la auditoría, se establece el objetivo y el alcance de responsabilidad del auditor con el cliente y el tipo de dictamen que emitirá.

NIA 4 Planeación. Esta norma aplica el proceso de planeamiento de la auditoría para estados financieros y también de otra información financiera, el primer punto clave es desarrollar un plan general con el alcance, y el segundo es un programa de auditoría que muestre la naturaleza, oportunidad y alcance de los procedimientos de auditoría.

NIA 5 Utilización del trabajo de otros auditores. Esta norma se aplica cuando el auditor independiente, utiliza el trabajo de otro auditor independiente con respecto a estados financieros de divisiones, sucursales, subsidiarias o compañías asociadas incluidas en los estados financieros de la entidad.

NIA 6 Evaluación del riesgo y del control interno. Permite dar una guía para el estudio y comprobación del sistema de control interno, en la evaluación de los riesgos inherentes y de control y utilizar esta evaluación para el diseño de procedimientos sustantivos y el auditor disminuya el riesgo de detección a un nivel aceptable.

NIA 7 Control de calidad del trabajo de auditoría. El propósito de esta norma es los procedimientos que el auditor debe cumplir en lo que se refiere al delegar el trabajo a sus asistentes y también los procedimientos que debe adoptar la firma auditora para la presentación de calidad sobre los trabajos que realiza.

NIA 8 Evidencia de auditoría. A través de los procedimientos sustantivos se debe obtener evidencia de la integridad, exactitud y validez de la información y existen dos tipos de pruebas, la primera es el detalle de transacciones y de los saldos, análisis de ratios y tendencias significativas que incluye fluctuaciones y partidas inusuales.

NIA 9 Documentación. El auditor debe documentar toda la evidencia que resulte importante y debe hacerlo de conformidad con los principios básicos de las NIAs, aquí se incluyen los papeles de trabajo que ayudan a planear, ejecutar y supervisar la auditoría es la evidencia que sustenta el trabajo del auditor.

NIA 10 Utilización del trabajo de un auditor interno. Se refiere a que el auditor independiente emite su opinión, alcance y procedimientos de auditoría y puede

utilizar o servirle de gran manera la información del auditor interno al examinar la información financiera.

NIA 11 Fraude y error. Esta norma discute la responsabilidad del auditor por la detección de distorsiones materiales ocasionadas por fraude o error en una auditoría de estados financieros y que procedimientos debe aplicar cuando encuentre este tipo de circunstancias.

NIA 12 Procedimientos analíticos. El propósito es analizar los índices y tendencias importantes, incluyendo las fluctuaciones y partidas poco usuales resultantes.

NIA 13 El dictamen del auditor sobre los estados financieros. El fin de esta norma es orientar a los auditores sobre el contenido y la forma del dictamen emitido en relación a la auditoría realizada.

NIA 14 Otra información en documentos de estados. El propósito es proporcionar orientación sobre la otra información sobre la cual el auditor no tiene la obligación de opinar.

NIA 15 Auditoría en un ambiente P E D (procesamiento electrónico de datos). El objetivo de esta norma es cumplir los principios básicos de una auditoría en un ambiente PED, es decir existe un ambiente PED cuando en el procesamiento de la información financiera interviene un computador.

NIA 16 Técnicas de auditoría con ayuda del computador. El propósito de esta norma establecer el tipo de software que se utiliza para una auditoría y cuáles son las técnicas de auditoría que se aplican con el uso de computadoras.

NIA 17 Entidades vinculadas. El propósito de esta norma es proporcionar procedimientos que el auditor debe aplicar para la obtención de evidencia adecuada en las entidades vinculadas y las transacciones con dichas entidades.

NIA 18 Utilización del trabajo de un experto. El objetivo de esta norma es proporcionar los lineamientos con relación a la responsabilidad del auditor en la utilización del trabajo de un experto como evidencia de auditoría y también los procedimientos que debe considerar al utilizar dicha evidencia.

NIA 19 Muestreo de auditoría. El objetivo de esta norma es identificar los factores que el auditor debe considerar cuando diseña y selecciona la muestra así como la evaluación de los resultados sobre los procedimientos de auditoría aplicados.

NIA 21 Hechos posteriores a la fecha del balance general. Esta norma proporciona información sobre la fecha del dictamen del auditor, su responsabilidad con hechos que surgen después de la fecha del balance general y también sobre el descubrimiento de hechos posteriores a su dictamen.

NIA 22 Manifestaciones de la gerencia. Se puede determinar como evidencia de auditoría las manifestaciones de la gerencia, el auditor debe conocer los procedimientos para evaluar y documentar dicha información y a su vez esta información debe ser respaldada por escrito.

NIA 23 Empresa en Marcha. El propósito que debe tener el auditor en esta norma es verificar que se cumple con los principios de empresa en marcha de tal forma que pueda identificar si la empresa puede o no dar continuidad a su negocio.

NIA 24 Dictamen del auditor con fines especiales. Es el dictamen del auditor diferente a la NIA13 y lo emite cuando: existen estados financieros aceptables preparados de manera distinta a las NIC, elementos de cuentas o cuentas específicas, cumplimientos de compromiso contractuales y estados financieros resumidos.

NIA 25 Materialidad y riesgo de auditoría. Esta norma define y describe los conceptos de materialidad y riesgo de auditoría su interrelación para planear y conducir una auditoría así como evaluar los resultados de los procedimientos.

NIA 26 Auditoría a estimados contables. El fin de esta norma es obtener una razonable certidumbre acerca de la propiedad de las estimaciones contables contenidas en la información financiera.

NIA 27 Examen de información financiera pre elaborada. La información financiera pre elaborada se basa en supuestos o presunciones de hechos futuros para que la entidad pueda tomar decisiones basadas en ese hecho, sirve como una herramienta de administración y también para terceras personas como informes e proyección para futuros ingresos de capital o inversiones.

NIA 28 Compromiso de la primera auditoría y saldo de apertura. En esta norma el auditor debe obtener evidencia suficiente y competente sobre los saldos de apertura que no contengan distorsiones de manera material en los estados financieros, los saldos del año anterior han sido correctamente arrastrados al año en curso y se han aplicado políticas contables apropiadas.

NIA 29 Estimaciones de riesgo inherente y de control y su impacto en los procedimientos sustantivos. Esta norma provee orientación al auditor en la estimación de los riesgos inherentes y de control para diseñar pruebas sustantivas para disminuir el riesgo de detección a un nivel aceptable.

NIA 30 Conocimiento de los negocios. El auditor debe conocer un conocimiento suficiente del negocio para que le permita identificar entender los eventos y transacciones que a juicio del auditor pueda tener un efecto significativo sobre los estados financieros el examen o el informe.

NIA 31 Consideración de las leyes y regulaciones en una auditoría de estados financieros. El auditor debe reconocer que la falta de cumplimiento de la entidad con las leyes y regulaciones puede afectar significativamente los estados financieros, en esta norma se refiere a actos de omisión o actos ilegales efectuados intencional o no intencionalmente por la entidad auditada.

NIA 32 Principios básicos que rigen un compromiso de revisión. Es el compromiso por el cual el auditor se compromete a aplicar procedimientos que van a suministrar un moderado nivel de certidumbre sobre la información financiera y este nivel de certidumbre debe ser menor que el que suministra la auditoría.

NIA 33 Revisión de los estados financieros. Permite al auditor expresar en base a los procedimientos realizados sobre toda la evidencia de auditoría si ha encontrado o no elementos que le permitan inferir si toda la información revisada no presenta una certeza razonable de conformidad con las prácticas contables.

NIA 34 El compromiso de aplicación de los procedimientos acordados. Se basa en la aplicación de los principios básicos del auditor al realizar una auditoría estos son: integridad, objetividad, confidencialidad, habilidad y competencia, documentación, planeamiento y evidencia, también debe describir la forma y contenido del informe con los hallazgos con relación a los compromisos por el cumplimiento de procedimientos acordados.

NIA35 Compromiso de compilación de información financiera. En esta norma el auditor se compromete a utilizar su pericia contable para centralizar y simplificar información tomada al detalle, haciéndola manejable y comprensible sin que exista la posibilidad de comprobar las afirmaciones de dicha información.

2.6 Firmas de auditoría del cantón Quito

Para el estudio de los sistemas de información que utilizan las firmas auditoras del cantón Quito se tomó como población en base a la información proporcionada por la superintendencia de compañías y son 298 firmas auditoras, de los cuales 113 se identifican como firmas auditoras y 185 auditores independientes para nuestro estudio nos basamos en las firmas auditoras.

Para la obtención de la muestra se usa la fórmula de muestreo aleatorio simple la cual se aplica de la siguiente manera:

$$n = \frac{N\sigma^2Z^2}{(N-1)e^2 + \sigma^2Z^2}$$

Dónde:

n = el tamaño de la muestra.

N = tamaño de la población.

σ = Desviación estándar de la población que por lo general tiene un valor de 0,5.

Z = Valor del nivel de confianza del investigador en este 95% (1.96).

e = Límite aceptable de error muestral que generalmente varía entre el 1% (0,01) y 9% (0,09).

Para determinar el número de firmas auditoras a investigar del cantón Quito se aplica la fórmula de la siguiente manera.

$$n = \frac{N\sigma^2Z^2}{(N-1)e^2 + \sigma^2Z^2}$$

n = el tamaño de la muestra.

N = tamaño de la población (113).

σ = Desviación estándar de la población que por lo general tiene un valor de (0,5).

Z = Valor del nivel de confianza del investigador en este 95% (1.96).

e = Límite aceptable de error muestral (0,06).

$$n = \frac{(113)(0,5)^2(1,96)^2}{(113-1)(0,06)^2 + (0,5)^2(1,96)^2}$$

$$n = 79,58$$

$$n = 80$$

Por lo tanto se hará el estudio para 80 firmas auditoras.

A continuación se muestran las firmas de auditoría del cantón Quito:

Tabla 4.
Firmas de auditoría del cantón Quito.

N°.	NOMBRE	CIUDAD
1	Abadhel Cia. Ltda.	Quito
2	Acevedo y asociados Cia. Ltda.	Quito
3	Adico auditores y contadores independientes Cia. Ltda.	Quito
4	Advisory & consulting auditores Cia. Ltda.	Quito
5	Aena, auditores y consultores Cia. Ltda.	Quito
6	Aguirre & asociados Cia. Ltda.	Quito
7	Aliro morales & asociados contadores públicos-auditores-consultores Cia. Ltda.	Quito
8	Almeida & asociados Cia. Ltda.	Quito
9	Andrade Guayasamín Cia Ltda.	Quito
10	Apoyo internacional gordillo endara & asociados Cia. Ltda.	Quito
11	Arbitros peritos auditores s.a. arpausa	Quito
12	Asesores asociados equitycorp Cia. Ltda.	Quito
13	Asesores tributarios legales astrileg Cia. Ltda.	Quito
14	Asesores tributarios legales contables atrilco Cia. Ltda.	Quito
15	Assurance & services auditores Cia. Ltda.	Quito
16	Atig auditores y asesores Cia. Lda.	Quito
17	Attest auditores & asociados Cia. Ltda.	Quito
18	Audiassurance Cia. Ltda.	Quito
19	Audicomex auditoría, comercio, exportación e importación Cia. Ltda.	Quito
20	Audisupport Cia. Ltda.	Quito
21	Auditbureau Ecuador Cia. Ltda.	Quito
22	Auditing support Cia. Ltda.	Quito
23	Auditora empresarial mosquera vega y asociados Cia. Ltda.	Quito
24	Auditora villavicencio & asociados Cia. Ltda.	Quito
25	Auditores asesores financieros y tributarios attesting group Cia. Ltda.	Quito
26	Auditores consultores v.m.r. del Ecuador Cia. Ltda.	Quito
27	Auditores y abogados asociados lawcontrollers Cia. Ltda.	Quito

28	Auditoria y gestión legal, cateleg Cia. Ltda.	Quito
29	Auditory & accounts s.a. adaccounts	Quito
30	Auditricont Cia. Ltda.	Quito
31	Auditsolutions soluciones de auditoría integral Cia. Ltda.	Quito
32	Auditsolver auditores y contadores Cia. Ltda.	Quito
33	Aurea co cpas Cia. Ltda.	Quito
34	Baker tilly Ecuador Cia. Ltda.	Quito
35	Batallas & batallas auditores y asesores Cia. Ltda.	Quito
36	Bcgbusiness consulting group del Ecuador Cia. Ltda.	Quito
37	Bdo Ecuador Cia. Ltda.	Quito
38	Bermudez & asociados Cia. Ltda.	Quito
39	Business development services imperium bisdevelopserv Cia. Ltda.	Quito
40	Castro mora asociados Cia. Ltda.	Quito
41	Chavez, granados, mancheno, regalado, audifins Cia. Ltda.	Quito
42	Cimaudidores Cia. Ltda.	Quito
43	Compañía de servicio de auditoría outcontrol Cia. Ltda.	Quito
44	Compañía ecuatoriana de capacitación, auditoría y asesoría cedcaya Cia. Ltda.	Quito
45	Conaudin, contabilidad y auditoría integral Cia. Ltda.	Quito
46	Consultora Fausto Ávila asociados Cia. Ltd.	Quito
47	Consultora gabela Cia. Ltda.	Quito
48	Consultora Jiménez espinosa Cia. Ltda.	Quito
49	Consultores naranjo Holguín Cia. Ltda.	Quito
50	Consultores, auditores loya & asociados Cia. Ltda.	Quito
51	Contaprex Cia. Ltda. (profesionales contables & auditores externos)	Quito
52	Delgado bolaños & asociados-auditores Cia. Ltda.	Quito
53	Deloitte & touche Ecuador Cia. Ltda.	Quito
54	Dendritol s.a.	Quito
55	Dr. Eladio Galarza torres, auditores y consultores asociados egatol Cia. Ltda.	Quito

56	Egas daza y asociados Cia. Ltda.	Quito
57	Ernest & young ecuador e&y Cia. Ltda.	Quito
58	Especialistas en consultoria, auditoría y tributacion escayt Cia. Ltda.	Quito
59	Estudio superior de tecnica contable e.s.u.t.e.c.o. c ltda	Quito
60	Felix montalvo & asociados felmon Cia. Ltda.	Quito
61	Fpsaudytors & asociados Cia. Ltda.	Quito
62	Freire hidalgo auditores s.a.	Quito
63	Futurefocus consulting Cia. Ltda.	Quito
64	Ganzbed auditores s.a.	Quito
65	Grant thornton dbrag ecuador Cia. Ltda.	Quito
66	Grupo corporativo de asesores y auditores garisa s.a.	Quito
67	Guerra y asociados Cia. Ltda.	Quito
68	Guerraudit consultores Cia. Ltda.	Quito
69	Hansen holm y Cia. Ltda.	Quito
70	Ifs integral financial solutions Cia. Ltda.	Quito
71	Illengi Cia. Ltda.	Quito
72	Ivan iglesias & asociados Cia. Ltda.	Quito
73	J. Patricio lincango consulauditores Cia. Ltda.	Quito
74	Jetvile associates Cia. Ltda.	Quito
75	Jorge zapata lara jezl contadores y auditores Cia. Ltda.	Quito
76	Kreston audit services ecuador Cia. Ltda.	Quito
77	Latinaudit latinoamericana de auditores Cia. Ltda.	Quito
78	Maldonado acosta estrella auditores consultores Cia. Ltda.	Quito
79	Martinez Chávez y asociados Cia. Ltda.	Quito
80	Mauricio arroyo & asociados consultores Cia. Ltda.	Quito
81	Mba management & business advisory Cia. Ltda.	Quito
82	Melo-bermeo y asociados auditores externos Cia. Ltda.	Quito
83	Micelle Cia. Ltda.	Quito
84	Morales & asociados Cia. Ltda.	Quito
85	Morgan internacional auditores Cia. Ltda.	Quito
86	Núñez serrano y asociados Cia. Ltda.	Quito

87	Paez, florencia & co Cia. Ltda.	Quito
88	Paredes santos & asociados Cia. Ltda.	Quito
89	Partner auditing auditores internacional Cia. Ltda.	Quito
90	Partnerdealings Cia. Ltda.	Quito
91	Pharosauditores externos Cia. Ltda.	Quito
92	Pricewaterhousecoopers del Ecuador Cia. Ltda.	Quito
93	Proaudit Cia. Ltda.	Quito
94	Proverbium, asesores gerenciales Cia. Ltda.	Quito
95	Rosero carrera & asociados Cia. Ltda.	Quito
96	Ruiz vega cevallos enterprise & asociados ruivecsa Cia. Ltda.	Quito
97	Russell bedford Ecuador s.a.	Quito
98	Sanchez & sanchez consultores Cia. Ltda.	Quito
99	Sanchez orbe auditores independientes Cia ltda	Quito
100	Santamaria & asociados auditores independientes Cia. Ltda.	Quito
101	Sbv auditores asociados Cia. Ltda.	Quito
102	Servicesmaas Ecuador Cia. Ltda.	Quito
103	Servicios de auditoría externa saex Cia. Ltda.	Quito
104	Servicios de auditoría y controles operativos Cia. ltda sayco	Quito
105	Servicios integrados de contabilidad y auditoría intercauser Cia. Ltda.	Quito
106	Signexternal auditors Cia. Ltda.	Quito
107	Solnopro soluciones no problemas s.a.	Quito
108	Taxgold auditores Cia. Ltda.	Quito
109	Teamauditores Cia. Ltda.	Quito
110	Vs&p auditum s.a.	Quito
111	Willi bamberger & asociados Cia. Ltda.	Quito
112	Wilson & wilson Cia. Ltda.	Quito
113	Wolfxcat s.a. financial management & tax consulting	Quito

Nota: Exposición de las firmas de auditoría del cantón Quito.

CAPÍTULO 3

METODOLOGÍA DE INVESTIGACIÓN

A través del presente capítulo se presentará el diseño de la investigación que se va a realizar así como los métodos para poder recolectar la información y su presentación posterior, también se detallará la encuesta a ser proporcionada a las firmas auditoras del cantón Quito y que nos demostrará todos aquellos datos que necesitamos para la investigación.

3.1 Diseño de la investigación

La investigación se basa en un diseño no experimental porque no se realizarán experimentos para comprobar las variables en conjunto con los indicadores por lo tanto se lo define así: “Es la investigación que se realiza sin manipular las variables lo que se hace es la observación de los fenómenos tal cual se dan en su contexto natural, para posteriormente su análisis”. (Gómez, 2006, pág. 102). De esta manera analizaremos la información recolectada tal y como se presenta sin manipular sus variables además que se realiza posterior a su ejecución de tal forma que se pueda explorar en su todo su contexto la información en las áreas en las que se aplica.

A continuación se realiza una investigación exploratoria que permiten indagar en todos los aspectos de la información en un tiempo y espacio pero para adentrarnos en este tema en primera instancia describiremos los tipos de investigación no experimental que las describe (Sampieri, 2006, pág. 208). En su libro así.

Investigación no experimental.

- Transeccional
- Longitudinal

En el tipo de investigación no experimental transeccional pueden ser de tres tipos estos son:

Diseños transeccionales exploratorios. “Se trata de una aproximación de manera inicial al fenómeno a investigar”. (Gómez, 2006, pág. 103). En este diseño lo que se trata de obtener es una visión general del objeto a investigar, de esta manera recogemos la información que necesitamos y que nos permita formarnos criterio adecuado de la situación actual de la organización sobre el tema que necesitamos investigar.

Diseños transeccionales descriptivos. “Su objetivo es la indagación en la incidencia de valores que se manifiestan en una o más variables esto dentro de un enfoque cuantitativo o proporcionar una visión de un fenómeno se los describe dentro de un enfoque cualitativo”. (Gómez, 2006, pág. 103). En este diseño lo que se hace es indagar y recoger información de un evento o situación ocurrido en un tiempo determinado, el objetivo es verificar como las variables han mostrado cambios a través de la diferentes situaciones que se puedan presentar hablando del enfoque cuantitativo pero desde el enfoque cualitativo describir la situación o el fenómeno nos permite tener las cualidades propias de ese acontecimiento.

Diseños transeccionales correlacionales-causales. “Describen la relación entre dos o más conceptos variables o categorías en un momento determinado”. (Gómez, 2006, pág. 103). A través de este diseño lo que se busca es la relación entre enfoques cuantitativos (medición) y cualitativos (análisis), por ende existirá una relación entre sus variables que no necesariamente contengan una asociación por las causas que lo generaron.

En el tipo de investigación no experimental longitudinal existen tres tipos de diseños y se los detalla de la siguiente forma.

Diseño no experimental longitudinal de tendencia. “Se realiza un estudio de los cambios en las variables o de sus relaciones a través del transcurso del tiempo de una población en general”. (Hurtado León & Toro Garrido, 2007, pág. 103). En este caso lo que se debe hacer es realizar mediciones a través del tiempo de la población o de una muestra que puede ser muy representativa cada momento que se desea hacer las mediciones.

Diseño no experimental longitudinal de evolución de grupo. “En este tipo de diseños lo que se busca es examinar los cambios a través del tiempo en una parte o subgrupo de la población”. (Hurtado León & Toro Garrido, 2007, pág. 103)

Diseño no experimental longitudinal de panel. “En este diseño la muestra siempre será la misma de manera que se tiene la ventaja de que se conocen los cambios individuales y los grupales a través del tiempo”. (Hurtado León & Toro Garrido, 2007, pág. 103)

Una desventaja de este diseño es que se mantiene la misma muestra a través del tiempo y pueden existir cambios significativos en las variables que lo conforman y no examinar o dejar de lado aquellos puntos que pueden ser importantes.

Una vez conocido los tipos de investigación no experimental nos centraremos en el tipo de investigación transeccional descriptiva porque la utilizaremos en nuestro proceso de investigación, los cambios que se producen como actúan y como se presentan los sistemas de información en las firmas auditoras del cantón Quito como estas modificaciones pueden afectar en la toma de decisiones y como se puede actuar para mantener un control sobre dichas decisiones es decir que consecuencias conlleva mantener un sistema de información adecuado a las necesidades de la organización.

3.2 La encuesta

Se la define como una técnica de primaria de obtención de información sobre la base de un conjunto objetivo, coherente y articulado de preguntas que garantiza que la información proporcionada por la muestra analizada mediante métodos cuantitativos que pueden arrojar errores pero también el nivel de confianza de una población. (Grande & Abascal, 2005, pág. 14).

En el concepto lo que se busca es el análisis de la información proporcionada por una muestra que nos refleje un nivel de confianza aceptable que nos permita poder emitir

una opinión de acuerdo a los resultados obtenidos que conlleven a una futura toma de decisiones.

3.2.1 Ventajas de la utilización de encuestas

Existen algunas ventajas por el uso de encuestas así podemos identificar la que más se adecúe a las necesidades, así:

Estandarización. Nos indica que todas las preguntas se harán a todos los elementos de la muestra lo que implica homogeneidad de la información.

Facilidad de administración. Significa que la persona encuestada solo se va a limitar a leer y contestar las preguntas.

Facilidad de tratamiento de datos. Significa que cada pregunta esta codificada y puede convertirse o tabularse a una expresión cualitativa y convertirla en cuantitativa de ser el caso para poder interpretarla con descripciones y a su vez estas con su valor numeral.

Obtención de información adicional. Al realizar una encuesta se puede obtener algún tipo de información relativa a su negocio, puede ser sus asociaciones, convenios, premios y responsabilidad social, etc.

Posibilidad de hacer estudios parciales. Por medio de la encuesta se puede hacer un estudio imponiendo condiciones en las preguntas para conocer la segmentación, imagen, posicionamiento en el mercado, etc.

3.3 El cuestionario. “Es un conjunto articulado y coherente de preguntas que nos permiten obtener toda la información que se necesita al realizar una investigación y tiene como función trasladar el objetivo de la investigación al realizar las preguntas concretas hacia el encuestado”. (Grande Esteban & Abascal Fernandez, 2009, pág. 189). Al revisar este concepto podemos inferir que el cuestionario que vamos a aplicar nos dará las respuestas correctas de aquello que queremos buscar, los aspectos

que necesitamos conocer y toda la información actual que nos permitirá emitir un criterio lógico para dar a conocer los resultados obtenidos.

3.3.1 Clases de preguntas. A continuación presentaremos algunas clases de preguntas y su criterio para la clasificación.

Tabla 5.
Clases de preguntas.

CLASES DE PREGUNTAS	
Criterio de Clasificación	Clases de preguntas
Libertad de elección de respuestas	Abiertas Cerradas Semicerradas
Cantidad de Respuestas y su relación	Dicotómicas Respuesta Múltiple Batería de preguntas
Fines de preguntas	Filtro Control Obtener información
Forma de realizarse	Directas Indirectas

Nota: Criterios de clasificación para los tipos de preguntas.

Ahora analizaremos cada clase de pregunta de acuerdo a las definiciones del autor antes mencionado:

3.3.1.1 Por la libertad de elección

Preguntas abiertas. Son preguntas que el encuestado responde libremente, sirve para encontrar posibles actitudes, motivaciones conductas, opiniones, etc.

Ejemplo.

1.-	¿Te gusta ir a caminar al parque?
2.-	¿Por qué te gusta el chocolate?

Preguntas cerradas. En este tipo de preguntas las respuestas están limitadas por una o varias alternativas resultan muy interesantes cuando no se requiere profundizar

mucho en un tema, por lo general lo único que se trata con este tipo de preguntas es solo recoger hechos.

Ejemplo.

1.-	¿Qué bebida te gusta tomar?
-----	-----------------------------

2.-	¿Qué tipo de comida te gusta comer?
-----	-------------------------------------

Preguntas Semicerradas. En este tipo de preguntas hay la posibilidad de encontrar alternativas cerradas y alternativas que el encuestado puede responder libremente.

Ejemplo.

1.-	¿Usted es mayor de edad?
Sí: <input type="checkbox"/> No <input type="checkbox"/>	
Si responde que sí: ¿Qué carrera la gustaría estudiar?	

2.-	¿Usted sabe conducir?
Sí: <input type="checkbox"/> No <input type="checkbox"/>	
Si responde que sí: ¿Qué clase de auto quisiera manejar?	

3.3.1.2 Por la cantidad de respuestas y su relación

Preguntas dicotómicas. Este tipo de preguntas solo existen dos tipos de alternativas y son mutuamente excluyentes, es decir solo puede haber una de las dos. Ejemplo: tiene automóvil o no, tiene hijos o no, estudia o no, etc.

Ejemplo.

1.-	¿Qué color prefiere?
Blanco: <input type="checkbox"/> Negro: <input type="checkbox"/>	

2.-	¿Ayer miró alguna película en el cine?	
Sí:	<input type="checkbox"/>	No: <input type="checkbox"/>

Preguntas con múltiples respuestas. Cuando se le presenta la interrogante el encuestado tiene la opción de responder con varias alternativas.

Ejemplo.

1.-	¿Qué tipos de deporte le gusta practicar?	
	fútbol	<input type="checkbox"/>
	tennis	<input type="checkbox"/>
	básquetbol	<input type="checkbox"/>
	natación	<input type="checkbox"/>
	atletismo	<input type="checkbox"/>

2.-	¿Qué tipos de película le gusta ver?	
	acción	<input type="checkbox"/>
	drama	<input type="checkbox"/>
	aventura	<input type="checkbox"/>
	terror	<input type="checkbox"/>
	infantil	<input type="checkbox"/>

Preguntas en batería. Son preguntas relacionadas con un mismo tema que se integran entre sí y además son complementarias.

Ejemplo.

1.-	¿Qué clase de vino le gusta tomar?	
Blanco:	<input type="checkbox"/>	Tinto: <input type="checkbox"/>

2.-	¿En qué lugar compra el vino?		
Tiendas:	<input type="checkbox"/>	Bares:	<input type="checkbox"/>
Market:	<input type="checkbox"/>	Otro:	<input type="checkbox"/>

3.-	¿Con que frecuencia toma vino al mes?	
Una vez al mes	<input type="checkbox"/>	
Dos veces al mes	<input type="checkbox"/>	
Tres veces al mes	<input type="checkbox"/>	
Cada fin de semana	<input type="checkbox"/>	

3.3.1.3 Por los fines de respuesta

Preguntas filtro. Se las denomina así porque a través de la respuesta de esa pregunta se puede excluir o incluir a la siguiente pregunta.

Ejemplo.

1.-	¿Usted fuma?	
Sí:	<input type="checkbox"/>	No: <input type="checkbox"/>

2.-	¿Qué tipo de cigarrillo de gusta fumar?		
Blanco:	<input type="checkbox"/>	Menta:	<input type="checkbox"/>
Rojo:	<input type="checkbox"/>	Otro:	<input type="checkbox"/>

3.-	¿Con que frecuencia fuma a la semana?	
Una vez	<input type="checkbox"/>	
Dos veces	<input type="checkbox"/>	
Tres veces	<input type="checkbox"/>	
Todos los días.	<input type="checkbox"/>	

Preguntas de control. Tienen como objetivo verificar la coherencia de las respuestas proporcionadas por la persona encuestada.

Ejemplo.

1.-	¿Usted estudia una carrera universitaria?	
Sí:	<input type="checkbox"/>	No: <input type="checkbox"/>

2.-	¿Qué tipo de modalidad estudia?	
Presencial	<input type="checkbox"/>	Distancia. <input type="checkbox"/>
Semipresencial	<input type="checkbox"/>	Otro: <input type="checkbox"/>

3.-	¿Con que frecuencia asiste a clases a la semana?	
Una vez	<input type="checkbox"/>	
Dos veces	<input type="checkbox"/>	
Tres veces	<input type="checkbox"/>	
Todos los días.	<input type="checkbox"/>	

3.3.1.4 Por la forma de realizarse

Preguntas directas. Se formulan para tener solo una sola respuesta, esta a su vez puede ser dicotómica y cerrada.

Ejemplo.

1.-	¿A usted le gusta el inglés?	
Sí:	<input type="checkbox"/>	No: <input type="checkbox"/>

1.-	¿Qué idioma le gustaría aprender?
	francés
	portugués
	alemán
	latín
	otro

Preguntas indirectas. Son formuladas en el caso de que la respuesta sea difícil de obtenerla o para conocer si la persona encuestada tiene el conocimiento para responderla.

Ejemplo.

1.-	¿Me gustaría saber cómo te llamas?
-----	------------------------------------

2.-	¿Me gustaría saber que hace en su tiempo libre?
-----	---

Partiendo del hecho de que el cuestionario nos sirve para recolectar información en nuestro presente trabajo de investigación utilizaremos principalmente preguntas, abiertas, cerradas, semicerradas porque en primera instancia vamos a recolectar información general luego de apoco incrementaremos el nivel de intensidad de la preguntas hasta que el encuestado nos responda lo que queremos saber, así mismo expondremos tipos de preguntas de selección múltiple, con filtro y de control para comprobar que las respuestas guardan coherencia con las respuestas descritas con anterioridad.

3.4 Planteamiento de la hipótesis

El proceso de recolección de información confiable y segura permite que sea mayor el efecto y la importancia en la toma de decisiones para las empresas auditoras a través del uso de sistemas de información.

En esta hipótesis analizamos lo que se refiere a la información la misma que debe ser confiable y oportuna porque de ella depende la toma de decisiones, de esta manera se

garantiza la eficacia y eficiencia de las operaciones que se mantienen bajo el control de los sistemas de información un aspecto clave en este punto es que deben estar integrados a los procesos de la organización todos aquellos actores y usuarios que alimentan el sistema con las debidas seguridades y autorizaciones que les permitirán hasta cierto punto conocer los datos con los que se están ingresando al sistema, el segundo punto a consideración es organizar toda la información y que esta esté disponible para los directivos en cualquier momento pero ¿por qué?. Es necesario que en cualquier momento en el tiempo se pueda conocer cualquier falla o inconveniente en la manipulación, ingreso o tratamiento para que en ese momento tomar acciones correctivas que eliminen el riesgo que se presente en ese instante en la entidad.

3.5 Planteamiento de las variables

Variable independiente

- Información confiable y segura obtenida de los sistemas de información para la toma de decisiones.

Indicadores

- a) Personal que maneja el sistema: Su forma de organización, capacitación y funciones que tienen en la utilización del sistema.
- b) Instrumentación y control del sistema: Constituyen las normas, políticas y procedimientos que se derivan hacia el control del sistema como una fuente de datos confiables.

La variable independiente en este caso será la información que se ingresa en el sistema la misma que estará siempre disponible y respaldada, de esta manera se asegura el cumplimiento de seguridad de que los datos están siempre controlados y asegurados para sus posterior uso.

A través de los indicadores tenemos dos puntos a examinar.

El personal que maneja el sistema. Es en sí los usuarios que utilizan de forma periódica el sistema y por tanto deben contener las siguientes características.

Capacitación. Por lo general los sistemas informáticos una vez instalados contienen periódicamente actualizaciones, estas deben hacerse conocer al personal que maneja el sistema ya que es importante que conozcan los cambios que se produjeron para evitar errores en el tratamiento de la información.

Confidencialidad. Este factor es muy importante porque no debe divulgar la información que maneja con usuarios ajenos al entorno en el que se desenvuelve, por lo tanto los datos son privados con carácter restringido.

Seguridad. En este punto nos referimos al uso de las claves y el sentido de confidencialidad de las mismas porque no puede confiársele a otra persona ni mucho menos hacer uso de la misma para actividades ilegales dentro de la organización.

Respaldo de la información. Nos referimos a las copias de seguridad que se realizan del sistema, en qué tipo de medios se realizan los respaldos como por ejemplo en servidores en un edificio alejado, en el que se puede continuar las operaciones en caso de robo, sustracción, pérdida o un desastre natural, los medios físicos como discos magnéticos, memoria usb y el último recurso digital que se utiliza que es la Nube en la cual se puede respaldar toda la información que la organización desea y en el tiempo que esta lo requiera.

Instrumentación y control del sistema. Nos referimos a este indicador como una medición del control de los datos y de la información de la organización, es decir, como la entidad mantiene controles de seguridad para la información en caso de pérdida o sustracción de la misma, estos controles deben incluidos en los manuales de procedimientos y reglamentos que permitan sancionar el incumplimiento de las normas y generar una seguridad razonable de todos los procesos que conllevan la manipulación de la información.

Variable dependiente

- Importancia y Efecto de la aplicación de los sistemas de información para evitar situaciones de riesgo en la toma de decisiones.

Indicadores

- a) Normativa Existente: Se refiere hasta cuanto la normativa favorece a la mejora, implementación y mantenimiento del sistema de información.
- b) Evaluación de los sistemas de control: Ejecución de un conjunto de pruebas orientadas a descubrir errores en la salida de la información de manera aleatoria en el tiempo y en el lugar en que ocurra.

Mediante un análisis de la variable dependiente podemos entender que sin la información confiable y oportuna no se pueden tomar decisiones adecuadas y su efecto en las acciones a realizarse dependerá de la calidad de la información que se maneja. Ahora importancia al momento de trasladar los datos al sistema y que este sea el encargado de recopilar, organizar y entregar la información dependerá mucho también del nivel de capacitación de los usuarios así como de la tecnología que se utilice para el almacenamiento y respaldo porque esta es una base fundamental para la consecución de los objetivos propuestos por la organización.

A través de la verificación de los indicadores es importante controlar que el sistema de información este siempre actualizado, cumple con los estándares de seguridad vigentes, cumple con políticas de seguridad impuestas por los organismos de control y a su vez como esta normativa promueve el desarrollo de nuevas tecnologías para incrementar por ejemplo el nivel de seguridad del sistema, el fácil acceso a los datos por parte de los directivos, mantenimiento y control del sistema en cualquier momento para encontrar fallas y modificarlas, etc.

Otro aspecto muy importante es la evaluación a los sistemas de control a la información, entonces nos referimos a que debemos evaluar constantemente a los

sistemas de control de la información de la organización por ejemplo, evaluar el sistema antivirus, verificar que se encuentra actualizado, hacer pruebas con un virus infectado deliberadamente en el sistema, otra evaluación que se puede realizar es al manejo de la seguridad física del hardware por ejemplo controlar que los sistemas no puedan ser utilizados después de la jornada de trabajo sin previa autorización, controlar que el sistema que da acceso a los diferentes departamentos como las tarjetas o claves biométricas funcionan adecuadamente y como se debe reaccionar en caso de un siniestro para salvaguardar la información.

3.6 Selección de la muestra

A partir de este punto iniciaremos con la selección de la muestra que será objeto de nuestra investigación con el muestreo aleatorio estratificado, utilizando la siguiente fórmula:

$$\frac{113}{10} = 11.3$$

Por lo tanto el tamaño total de la población lo vamos a dividir en 10 grupos de 11 elementos cada uno, y de cada grupo se va a escoger los 8 primeros elementos para dejar excluidos a 3 y poder llegar al tamaño de la muestra que son 80 firmas ordenados alfabéticamente y que están presentes de la siguiente forma.

Tabla 6.
Firmas de auditoría del cantón Quito.

N°.	NOMBRE	CIUDAD
1	Abadhel Cia. Ltda.	Quito
2	Acevedo y asociados Cia. Ltda.	Quito
3	Adico auditores y contadores independientes Cia. Ltda.	Quito
4	Advisory & consulting auditores Cia. Ltda.	Quito
5	Aena, auditores y consultores Cia. Ltda.	Quito
6	Aguirre & asociados Cia. Ltda.	Quito
7	Aliro morales & asociados contadores públicos-auditores-consultores Cia. Ltda.	Quito
8	Almeida & asociados Cia. Ltda.	Quito
9	Andrade Guayasamín Cia Ltda.	Quito
10	Apoyo internacional gordillo endara & asociados Cia. Ltda.	Quito
11	Arbitros peritos auditores s.a. arpausa	Quito

12	Asesores asociados equitycorp Cia. Ltda.	Quito
13	Asesores tributarios legales astrileg Cia. Ltda.	Quito
14	Asesores tributarios legales contables atrilco Cia. Ltda.	Quito
15	Assurance & services auditores Cia. Ltda.	Quito
16	Atig auditores y asesores Cia. Lda.	Quito
17	Attest auditores & asociados Cia. Ltda.	Quito
18	Audiassurance Cia. Ltda.	Quito
19	Audicomex auditoría, comercio, exportación e importación Cia. Ltda.	Quito
20	Audisupport Cia. Ltda.	Quito
21	Auditbureau Ecuador Cia. Ltda.	Quito
22	Auditing support Cia. Ltda.	Quito
23	Auditora empresarial mosquera vega y asociados Cia. Ltda.	Quito
24	Auditora villavicencio & asociados Cia. Ltda.	Quito
25	Auditores asesores financieros y tributarios attesting group Cia. Ltda.	Quito
26	Auditores consultores v.m.r. del Ecuador Cia. Ltda.	Quito
27	Auditores y abogados asociados lawcontrollers Cia. Ltda.	Quito
28	Auditoria y gestión legal, cateleg Cia. Ltda.	Quito
29	Auditory & accounts s.a. adaccounts	Quito
30	Auditricont Cia. Ltda.	Quito
31	Auditsolutions soluciones de auditoría integral Cia. Ltda.	Quito
32	Auditsolver auditores y contadores Cia. Ltda.	Quito
33	Aurea co cpas Cia. Ltda.	Quito
34	Baker tilly Ecuador Cia. Ltda.	Quito
35	Batallas & batallas auditores y asesores Cia. Ltda.	Quito
36	Bcgbusiness consulting group del Ecuador Cia. Ltda.	Quito
37	Bdo Ecuador Cia. Ltda.	Quito
38	Bermudez & asociados Cia. Ltda.	Quito
39	Business development services imperium bisdevelopserv cia. Ltda.	Quito
40	Castro mora asociados Cia. Ltda.	Quito
41	Chavez, granados, mancheno, regalado, audifins Cia. Ltda.	Quito
42	Cimauditores Cia. Ltda.	Quito
43	Compañía de servicio de auditoría outcontrol Cia. Ltda.	Quito
44	Compañía ecuatoriana de capacitación, auditoría y asesoría cedcaya Cia. Ltda.	Quito
45	Conaudin, contabilidad y auditoría integral Cia. Ltda.	Quito
46	Consultora Fausto Ávila asociados Cia. Ltd.	Quito
47	Consultora gabela Cia. Ltda.	Quito
48	Consultora Jiménez espinosa Cia. Ltda.	Quito
49	Consultores naranjo Holguín Cia. Ltda.	Quito
50	Consultores, auditores loya & asociados Cia. Ltda.	Quito

51	Contaprex Cia. Ltda. (profesionales contables & auditores externos)	Quito
52	Delgado bolaños & asociados-auditores Cía. Ltda.	Quito
53	Deloitte & touche Ecuador Cia. Ltda.	Quito
54	Dendritol s.a.	Quito
55	Dr. Eladio Galarza torres, auditores y consultores asociados egatol Cia. Ltda.	Quito
56	Egas daza y asociados Cia. Ltda.	Quito
57	Ernest & young ecuador e&y Cia. Ltda.	Quito
58	Especialistas en consultoría, auditoría y tributación escayt Cia. Ltda.	Quito
59	Estudio superior de técnica contable e.s.u.t.e.c.o. Cia. Ltda.	Quito
60	Felix montalvo & asociados felmon Cia. Ltda.	Quito
61	Fpsaudytors & asociados Cia. Ltda.	Quito
62	Freire hidalgo auditores s.a.	Quito
63	Futurefocus consulting Cia. Ltda.	Quito
64	Ganzbed auditores s.a.	Quito
65	Grant thornton dbrag ecuador Cia. Ltda.	Quito
66	Grupo corporativo de asesores y auditores garisa s.a.	Quito
67	Guerra y asociados Cia. Ltda.	Quito
68	Guerraudit consultores Cia. Ltda.	Quito
69	Hansen holm y Cia. Ltda.	Quito
70	Ifs integral financial solutions Cia. Ltda.	Quito
71	Illengi Cia. Ltda.	Quito
72	Ivan iglesias & asociados Cia. Ltda.	Quito
73	J. Patricio lincango consuladores Cia. Ltda.	Quito
74	Jetvile associates Cia. Ltda.	Quito
75	Jorge zapata lara jezl contadores y auditores Cia. Ltda.	Quito
76	Kreston audit services Ecuador Cia. Ltda.	Quito
77	Latinaudit latinoamericana de auditores Cia. Ltda.	Quito
78	Maldonado acosta estrella auditores consultores Cia. Ltda.	Quito
79	Martinez Chávez y asociados Cia. Ltda.	Quito
80	Mauricio arroyo & asociados consultores Cia. Ltda.	Quito
81	Mba management & business advisory Cia. Ltda.	Quito
82	Melo-bermeo y asociados auditores externos Cia. Ltda.	Quito
83	Micelle Cia. Ltda.	Quito
84	Morales & asociados Cia. Ltda.	Quito
85	Morgan internacional auditores Cia. Ltda.	Quito
86	Nuñez serrano y asociados Cia. Ltda.	Quito
87	Paez, florencia & co Cia. Ltda.	Quito
88	Paredes santos & asociados Cia. Ltda.	Quito
89	Partner auditing auditores internacional Cia. Ltda.	Quito
90	Partnerdealings Cia. Ltda.	Quito

91	Pharosauditores externos Cia. Ltda.	Quito
92	Pricewaterhousecoopers del Ecuador Cia. Ltda.	Quito
93	Proaudit Cia. Ltda.	Quito
94	Proverbius, asesores gerenciales Cia. Ltda.	Quito
95	Rosero carrera & asociados Cia. Ltda.	Quito
96	Ruiz vega cevallos enterprise & asociados ruivecsa Cia. Ltda.	Quito
97	Russell bedford Ecuador s.a.	Quito
98	Sanchez & sanchez consultores Cia. Ltda.	Quito
99	Sanchez orbe auditores independientes Cia ltda	Quito
100	Santamaria & asociados auditores independientes Cia. Ltda.	Quito
101	Sbv auditores asociados Cia. Ltda.	Quito
102	Servicesmaas Ecuador Cia. Ltda.	Quito
103	Servicios de auditoría externa saex Cia. Ltda.	Quito
104	Servicios de auditoría y controles operativos Cia. ltda sayco	Quito
105	Servicios integrados de contabilidad y auditoría intercauser Cia. Ltda.	Quito
106	Signexternal auditors Cia. Ltda.	Quito
107	Solnopro soluciones no problemas s.a.	Quito
108	Taxgold auditores Cia. Ltda.	Quito
109	Teamauditores Cia. Ltda.	Quito
110	Vs&p auditum s.a.	Quito
111	Willi bamberger & asociados Cia. Ltda.	Quito
112	Wilson & wilson Cia. Ltda.	Quito
113	Wolfxcat s.a. financial management & tax consulting	Quito

Nota: Firmas de auditoría expuestas para análisis en la investigación.

3.7 Aplicación de métodos de investigación

Universidad Politécnica Salesiana Carrera de Contabilidad y Auditoría Encuesta a las Firmas Auditoras del Cantón Quito	
Datos de la Firma Auditora	Datos de la persona encuestada
Nombre de Firma:	Nombre:
Dirección:	Área en la que trabaja:
Dirección Web:	Fecha
<p>La presente encuesta está dirigida a las firmas auditoras del cantón Quito porque se desea conocer sobre sus <i>sistemas de información la importancia y efecto que tienen en la toma de decisiones</i>, de esta forma se emitirá informe de resultados en base a la investigación realizada.</p>	
ÁREA DE USUARIOS	
1.- ¿Existe un proceso estándar para crear y mantener las cuentas de usuario? _____ _____	
2.- ¿Existen perfiles de acceso que permite dar una seguridad al sistema? Sí: <input type="checkbox"/> No: <input type="checkbox"/> Si su respuesta es sí describirlo brevemente. _____ _____	
3.- ¿Existe un control para cada usuario de red de tal forma que se impida que un usuario pueda registrarse en otra maquina? Sí: <input type="checkbox"/> No: <input type="checkbox"/>	
4.- ¿Existe una revision periódica al usuario para verificar su actividad y evitar que trate de ingresar a sitios restringidos ? Sí: <input type="checkbox"/> No: <input type="checkbox"/>	
ÁREA DE SEGURIDAD	
5.- ¿Se entiende que debe existir copias de seguridad del sistema cuales son los medios disponibles? Discos duros <input type="checkbox"/> Otro: <input type="checkbox"/> Servidores <input type="checkbox"/> Medios magneticos <input type="checkbox"/> Especifique: Nube <input type="checkbox"/> _____	
6.- ¿Los sistemas de archivos están disponibles para todos los usuarios a través de la red? Sí: <input type="checkbox"/> No: <input type="checkbox"/>	
ÁREA INFRAESTRUCTURA	
7.- ¿Los sistemas de información (hardware y software) de las diferentes areas que utiliza la organización se encuentran asegurados ante cualquier eventualidad.? Sí: <input type="checkbox"/> No: <input type="checkbox"/>	

8.- ¿ Existe un manual de uso,políticas, normas de los sistemas así como tambien un reglamento que previene y sanciona el mal uso de los equipos computacionales?
 Sí: No:

ÁREA DE CAPACITACIÓN

9.- ¿Existe una politica que exige a la organización a capacitar a todos los usuarios sobre los cambios que se realizan en el sistema?
 Sí: No: Detalle brevemente : _____

10.- ¿Se considera la formación academica como un factor importante para el adecuado desempeño de las actividades dentro de la organización?
 Sí: No: ¿Porqué? _____

ÁREA DE ACTUALIZACIÓN

11.- ¿ Al realizar actualizaciones al sistema se realizan pruebas de control para verificar la estabilidad de dicha actualización?
 Si: No: ¿Cuál es la persona que certifica estas pruebas?

12.- ¿ Existe una política en la organización para instalar las actualizaciones de nuevas versiones?

TOMA DE DECISIONES

13.- ¿ El sistema de información del área contable es confiable y seguro por lo tanto permite evaluar las competencias de los usuarios que la utilizan?
 Sí: No: _____

14.- ¿Cuándo existe un problema de infraestructura es decir un daño o pérdida de algún equipo las medidas preventivas y correctivas se toman en ese instante indique el procedimiento?

15.- Cuándo se deben tomar decisiones sobre presupuestos,inversión, capital los realiza:

Administrador	<input type="checkbox"/>	Directorio	<input type="checkbox"/>
Representante legal	<input type="checkbox"/>	Junta de Accionistas	<input type="checkbox"/>
Gerente financiero	<input type="checkbox"/>	Otro:	<input type="checkbox"/> Espefique: _____

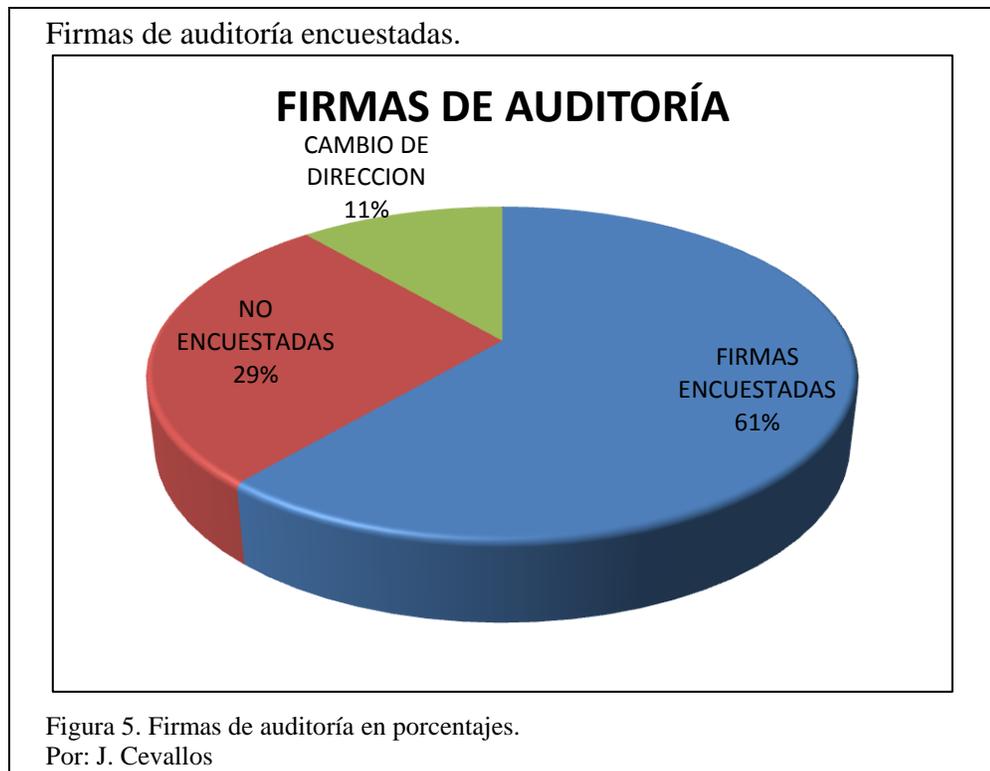
<p>16.- ¿Se han realizado cambios ultimamente en algun sistema de información que la organziación tiene y a su vez a mejorado la productividad o la calidad de servicio?</p> <p>_____</p> <p>_____</p>
<p>17.- ¿La actualización de conocimientos de los colaboradores o usuarios permite a la organización promover cargos cuando los conocimientos sean lo suficientemente amplios para poder aplicarlos?</p> <p>_____</p> <p>_____</p>
<p>18.- ¿Existe algun tipo de convenio con alguna empresa de seguridad para salvaguardar los activos físicos de la organización?</p> <p>Sí: <input type="checkbox"/> No: <input type="checkbox"/> Explique: _____</p> <p>_____</p> <p>_____</p>
<p>19.- ¿ Los reportes que se emiten en base a la información que emite el sistema estan parametrizados para que solo los puedan analizar los administadores, directores o gerentes?</p> <p>_____</p> <p>_____</p>
<p>20.- ¿ La interface del sistema permite una conexión amplia entre el usuario y el ordenador de tal forma que resulta facil la interpretacion y análisis de los datos ?</p> <p>Sí: <input type="checkbox"/> No: <input type="checkbox"/> Porqué: _____</p> <p>_____</p>

CAPÍTULO 4

ANÁLISIS DE LA INFORMACIÓN Y PRESENTACIÓN DE RESULTADOS

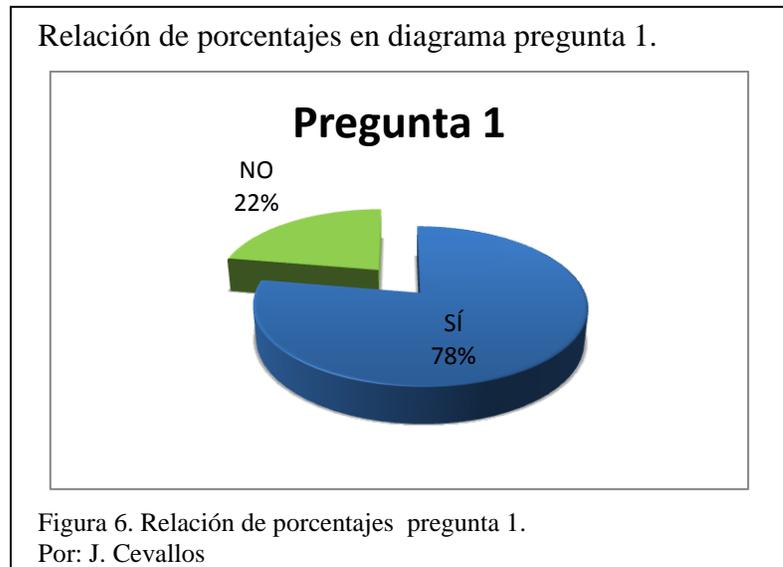
4.1 Análisis de la información

A través de nuestro proceso de investigación en primera instancia se logró determinar cuáles fueron las firmas auditoras que nos supieron entregar la información, que firmas no pudieron entregarnos los datos y también cuantas empresas se cambiaron de dirección, por lo tanto se las detalla así:



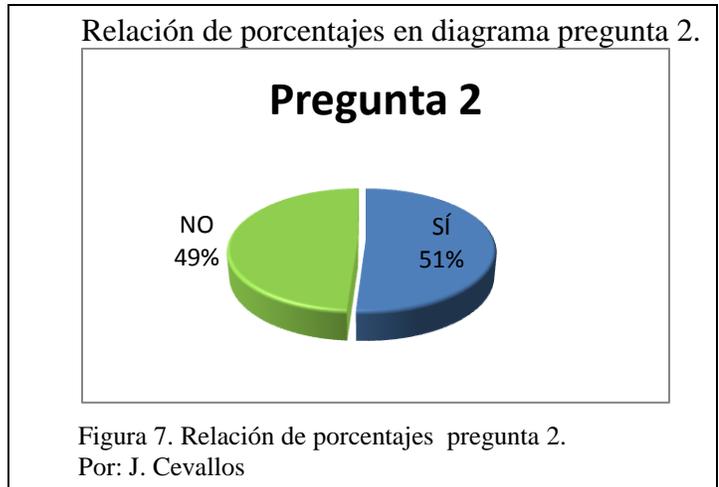
Continuando con el proceso de recolección de información se procederá al análisis de cada pregunta que se realizó a las firmas auditoras a través de la encuesta y que se detalla de la siguiente forma así:

Pregunta 1. ¿Existe un proceso estándar para crear y mantener las cuentas de usuario?



Analizando esta información se puede inferir que en un porcentaje mayor al 70% de firmas que se realizó maneja cuentas de usuario para las personas que laboran en la misma, esta es una medida de seguridad porque evita que los usuarios no autorizados utilicen un ordenador dedicado solo a un usuario. El otro porcentaje inferior al 23% que corresponde a que no utilizan cuentas de usuario representa un peligro para la organización porque cualquier persona ingrese para revisar o modificar archivos que son de uso solo de la entidad también puede ser que ingrese un experto en computación y robe información sensible o libere un código malicioso que permita transmitir toda la información a una estación o red diferente a la que se trabaja normalmente por lo tanto resulta de un gran riesgo no tener cuentas de usuario para hacer uso de los datos.

Pregunta 2. ¿Existen perfiles de acceso que permite dar una seguridad al sistema?



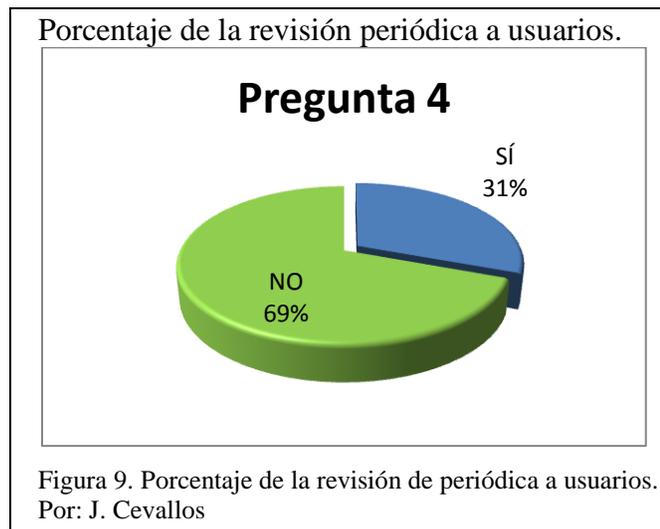
A través del presente gráfico se puede evidenciar que aproximadamente en un 51% de las firmas auditoras utiliza perfiles de acceso para dar un mayor control y seguridad al ingresar al sistema de trabajo porque es la principal herramienta que se utiliza de forma habitual, el restante 49% no tiene o no utiliza perfiles para el ingreso a software de aplicación esto representa un gran riesgo ya que limita la seguridad de usuarios a nada porque cualquier persona ya sea que pueda o no tener conocimiento sobre un tema en específico que se realice en la entidad puede tener acceso a toda la información de un usuario, ahora también existen algunas firmas que utilizan hojas de cálculo en Excel para realizar su trabajo es decir no cuentan con un software de aplicación para la realización de su trabajo por lo tanto este documento está adaptado a las necesidades de la organización que la utilice.

Pregunta 3. ¿Existe un control para cada usuario de red de tal forma que se impida que un usuario pueda registrarse en otra máquina?



Al analizar los resultados podemos inferir que solo un 37% de las firmas utilizan claves de usuario con privilegios de seguridad de tal forma que no se pueda registrar al mismo tiempo en otra máquina y utilizar los programas que utiliza habitualmente resulta de mucho beneficio por que cada usuario tiene límite de espacio de utilización en su disco, tiene acceso limitado a las aplicaciones, acceso limitado a la modificación edición o creación de archivos y algo muy importante adición de copias de seguridad en servidores, discos duros, medios magnéticos, la nube entre otros para el usuario registrado por tal motivo es importante además de los privilegios de cada usuario es también crear roles que permitan identificar los puntos de acceso al sistema. El 68% restante quiere decir que no utiliza el impedimento para el registro de un usuario en otra máquina por tanto resulta de una desventaja en tiempo real a la seguridad porque cualquier usuario puede hacer uso de otra máquina modificar datos cambiar registros y como no tiene roles definidos hurtar la información y pueda sacarle provecho para beneficio personal.

Pregunta 4. ¿Existe una revisión periódica al usuario para verificar su actividad y evitar que trate de ingresar a sitios restringidos?

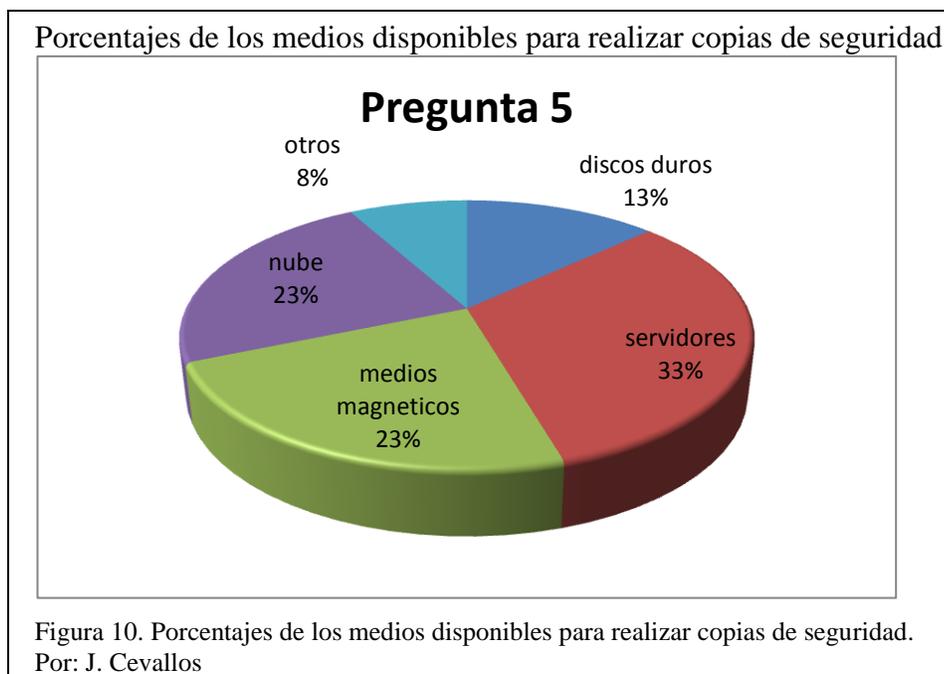


A partir del enfoque de seguridad de usuarios es imprescindible el monitoreo de seguridad de las actividades de los empleados de las organizaciones en el sentido de que siempre debe existir un control para evitar distracciones y minimizar el riesgo del espionaje corporativo ya que si se mantiene controlado al usuario se puede minimizar riesgos.

El 31 % de las firmas mantiene un nivel de seguridad alto porque a mayor seguridad menores riesgos, se preocupa por la salud y el bienestar de la organización está pendiente del control de los resultados y se mantiene alerta sobre a qué sitios puede acceder un empleado, que puede y no hacer en el aplicativo y obviamente tener un margen de error y de recuperación de información en caso de sustracción o pérdida o simplemente que se dediquen a realizar actividades que no son inherentes a su trabajo (ingresar al navegador de internet, enviar correos personales, descargar música, juegos etc.)

El 69% restante no mantienen un control sobre la actividad del usuario ya sea que tienen específicamente una aplicación o programa que debe realizar cada empleado o también porque confían de forma empírica de cada uno y por tanto no dan la importancia debida a todo el conjunto de procesos que se realizan en cada estación de trabajo así que es necesario incrementar el nivel de seguridad de la información con el uso de herramientas informáticas (software) y de forma proporcional seguir aumentando la seguridad de los recursos digitales puestos a disposición de todos.

Pregunta 5. ¿Se entiende que deben existir copias de seguridad del sistema cuales son los medios disponibles?



Ahora se presentan una relación de los medios utilizados por las firmas auditoras y el porcentaje que lo utilizan.

Tabla 7.
Medios disponibles utilizados por las firmas.

Tipo	Firmas	Tipo* firmas	%
1	11	11	22,45%
2	26	52	53,06%
3	12	36	24,49%
3	49	99	100,00%

Nota: Porcentaje de firmas que utilizan los medios disponibles

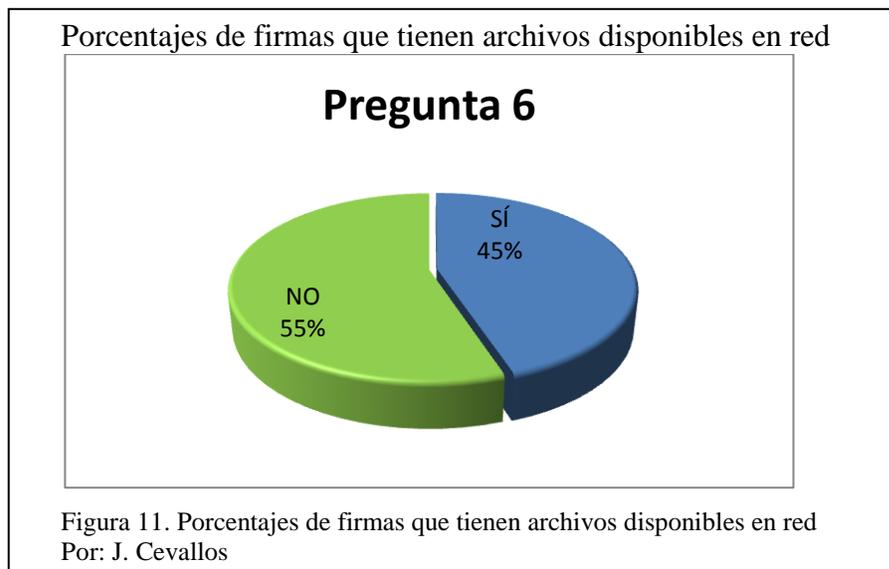
En esta pregunta podemos encontrar que el 13% de las firmas utiliza discos duros para respaldar la información es una buena opción porque se puede trasladar los datos a otro ordenador o servidor de una manera fácil y sencilla, en lo que se refiere a los servidores existe un 32% que si utilizan este medio para guardar la información es el más seguro porque en caso de siniestro perdida o hurto de la información siempre se va a tener en tiempo real los datos respaldados en un lugar alejado del habitual lugar trabajo.

En lo que corresponde a los medios magnéticos tenemos un 23% de aceptación que nos dice que este porcentaje utilizan el cd, dvd, pendrive, flash memory, microsd como medida de resguardo de los datos, así pues la nube comparte el mismo porcentaje y nos da a entender de que mucha de las empresas utilizan este tipo seguridad para sus datos porque resulta confiable y en tiempo real a través de internet poder tener acceso a la información, además porque no decirlo en cualquier parte del mundo estar siempre conectado y poder alimentar la información cuando se esté incrementando por ejemplo el número de clientes que tiene la organización en otros países, el numero de contacto e información de proveedores externos, las nuevas reformas o reglamentos por parte de nuestras subsidiarias, etc.

El 8 % restante tenemos otras opciones de copias de seguridad similares a la nube para respaldar la información como por ejemplo Box, Bropbox, icloud (usuarios de Apple para respaldar la información de sus dispositivos), Onedrive (usuarios de Microsoft) estos mecanismos permiten en tiempo real respaldar la información y se puede tener acceso a ella en cualquier momento.

También tenemos en la Tabla 7. un relación de las firmas que tienen un tipo, dos o tres medios para realizar backups a sus datos por lo tanto, el 22% de las organizaciones utilizan solo un tipo medio para realizar sus copias de seguridad en este caso vamos a realizar una relación de menor tipo de medios disponibles mayor el riesgo, el 53% de las firmas utiliza dos tipos de medios es decir que comparte el porcentaje de riesgo en un 50%, por último tenemos que el 24% de la firmas utiliza tres tipos de medios de seguridad que nos dice que a mayor medidas de seguridad menor es el riesgo de pérdida de la información.

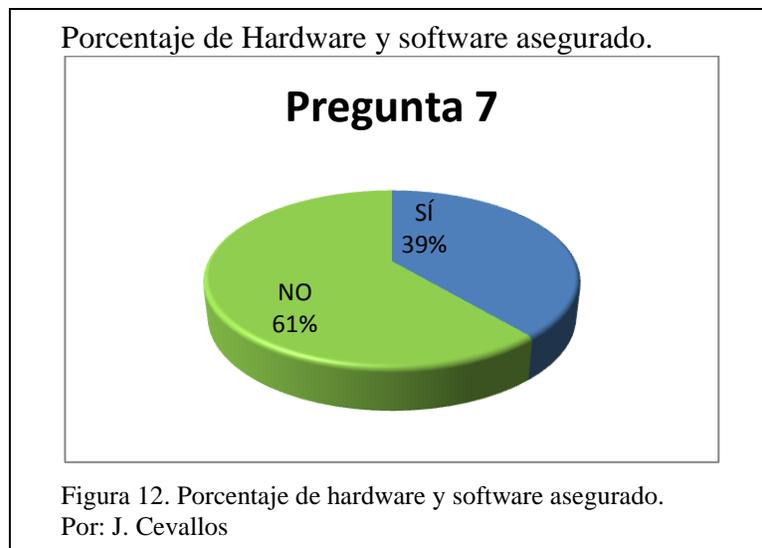
Pregunta 6. ¿Los sistemas de archivos están disponibles para todos los usuarios a través de la red?



Mediante el análisis de esta pregunta podemos identificar el riesgo que representa que todos los archivos estén disponibles para todos los colaboradores de la organización en la red que usan habitualmente en este caso 45%, cuando están definidos los roles de usuario se mantiene un control de las operaciones de cada persona pero también se mantiene una restricción a cada uno al implementar medidas de acceso que permite bloquear contenido restringido y sensible de la organización como pueden ser informes de la dirección, informes de presupuesto de los directores, políticas de nómina, reportes de inversionistas y proveedores entre otros usuarios operativos y que no tienen nada que ver con el proceso de toma de decisiones.

El restante 55% no mantiene los archivos disponibles para sus usuarios porque conocen la forma de no permitir el ingreso a estos datos por tanto se puede evitar la fuga de la información propia y de terceros, esto resulta de un gran beneficio ya que se puede aplicar como una política interna de la organización sobre la disponibilidad de los archivos y quién debe o no tener acceso.

Pregunta 7. ¿Los sistemas de información (hardware y software) de las diferentes áreas que utiliza la organización se encuentran asegurados ante cualquier eventualidad?



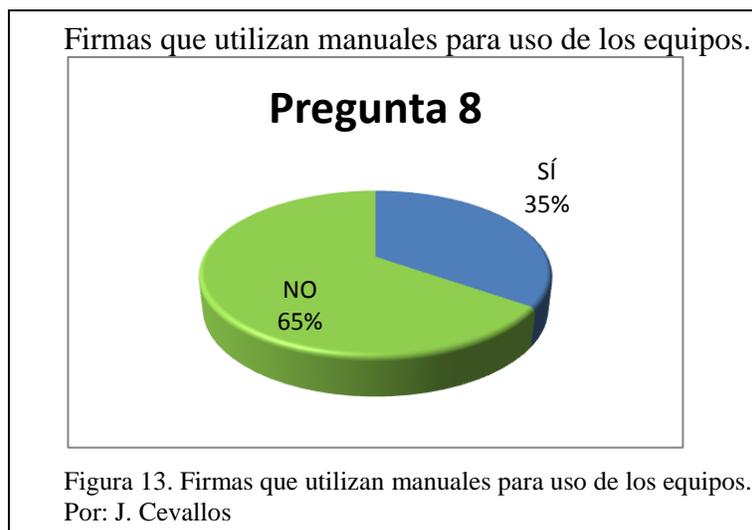
En esta pregunta podemos darnos cuenta el riesgo que corren muchas de las firmas de auditoría al no tener asegurados sus equipos en caso de que suceda algún evento inesperado y se vean afectados los sistemas informáticos en este caso un 61%, empecemos por el software en primera instancia se debe tener una copia de seguridad en los medios disponibles de tal forma que se pueda restaurar los datos en cualquier instante para verificar si los datos han sido afectados, otro punto importante es que si el software que se utiliza se llegara a dañar o estar siniestrado el proveedor o el departamento de sistemas debe tener la aplicación o el programa listo para poder instalarlo en la misma máquina o en otro ordenador para poder continuar con la operación del negocio, esto en caso en una eventualidad mínima por ejemplo un apagón no se guardaron los datos correctamente y tenemos que restaurarlos por lo tanto recurrimos a los backups y software de respaldo y si el evento ya es más grave

pues recurrir a todos los recursos disponibles para poder minimizar el impacto por la pérdida de información.

Por otro lado tenemos el hardware que es la herramienta que complementa al software y viceversa, en este caso tenemos la opción de restaurar los equipos inmediatamente en caso de un suceso leve si la empresa dispone de los recursos necesarios para solventar en ese instante los imprevistos, la otra opción es que si están asegurados pues esperar a la compañía de seguros la restitución de los mismos en los plazos establecidos por la póliza.

Con respecto al 39% de las firmas que si aseguran los equipos pues representa una gran ventaja competitiva ya que a mayor continuidad del negocio menor es el impacto económico que representa desembolsar por equipos que no sirven y que no están asegurados, también resulta un beneficio ya que muchos seguros brindan asistencia en el momento en que se suscita el siniestro, asistencia legal y otros beneficios que al no tener asegurado los sistemas se pierden.

Pregunta 8. ¿Existe un manual de uso, políticas, normas de los sistemas así como también un reglamento que previene y sanciona el mal uso de los equipos computacionales?



En la gráfica anterior identificar el riesgo que representa no asignar un manual o una política para el uso de sistemas en este caso el 65%, porque primero se corre el riesgo

de sustracción de equipos, de información, de recursos que la organización invierte para optimizar la capacidad de trabajo, el buen manejo debe verse reflejado en el cuidado que se le da a los implementos de trabajo proporcionados, también es importante recalcar que mal uso de los sistemas puede ocasionar en sanciones que perjudican el prestigio de la empresa por ejemplo error en los reportes a los organismos de control por descuido del personal, ocasiona de manera publica una amonestación escrita que genera un descontento en clientes, proveedores y la sociedad en general de tal forma que debe ser consiente el uso equipos y aplicaciones informáticas.

Continuando con el 35% restante nos da una clara muestra de la organización por mantener los equipos en buen estado, que reconoce que un buen equipo cuidado y actualizado representa en una mejora en la capacidad productiva así como una mejora en la resolución de problemas y toma de decisiones inherentes a la actividad, también propone un ambiente de trabajo adecuado por tanto existe una buena relación entre el usuario y le herramienta de trabajo.

Pregunta 9. ¿Existe una política que exige a la organización a capacitar a todos los usuarios sobre los cambios que se realizan en el sistema?

En esta pregunta se recogió algunos tipos de información por lo tanto se empezará a detallar el porcentaje de las empresas que no capacitan a los colaboradores cuando se realizan cambios en el sistema en este caso menos del 10% debido a las siguientes razones:

1. No utilizan sistemas complejos que en realidad necesitan pocos cambios o si se los realizan no necesitan capacitación sino que el usuario entiende perfectamente el cambio porque tiene un manejo constante del sistema.
2. Utilizan un sistema básico como es el Excel para sus procesos por tanto si se realiza un cambio ya sea importante o muy básico no afectaría en gran medida el desempeño del usuario al utilizar el programa.

3. Existen firmas de auditoría que están conformados de entre 5 a 10 personas que simplemente la persona que realiza cambios en su sistema ya sea que use un programa específico o una hoja de cálculo solo le sirve a la misma, por tanto no es necesario capacitar a todo el personal.

Ahora si se habla del porcentaje que capacita a sus usuarios sobre el cambio al sistema representa más de un 90% pero ¿cuál es la razón de esta situación?, obviamente la organización sabe que una persona capacitada en los cambios realizados ya sea que afecte directamente o no a sus procesos tiende a presentar una imagen de seguridad para cumplir los procedimientos con sus empleados se maneja de forma responsable y permite que el contenido de la información fluya para todos.

Pregunta 10. ¿Se considera la formación académica como un factor importante para el adecuado desempeño de las actividades dentro de la organización?

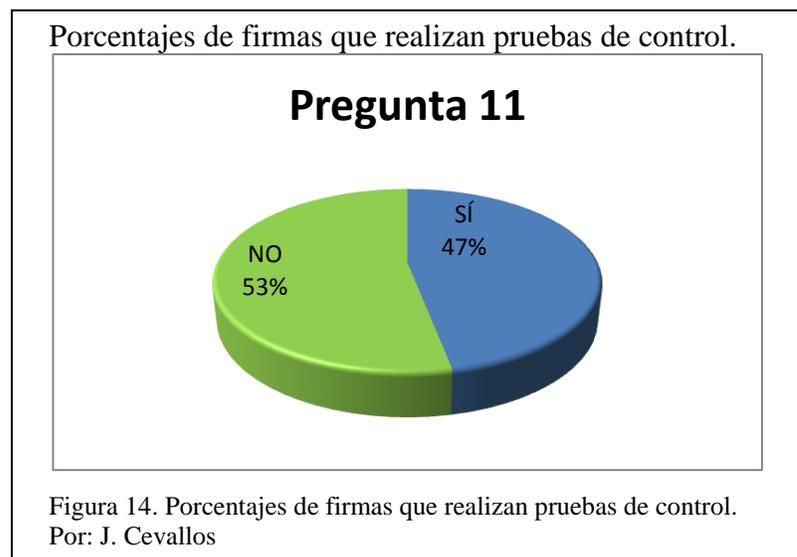
Con esta interrogante lo que logramos hacer es que el conocimiento teórico de los contenidos y elementos básicos de una persona que realiza su trabajo resultan imprescindibles para desempeñar de manera correcta las tareas encomendadas, partiendo de esto la mayoría de las firmas concuerda en la importancia de la capacitación como un factor fundamental para un buen desempeño en la organización debido a que da más seguridad a todos los procesos y se presenta como un respaldo de carácter teórico ante las exigencias de las herramientas tecnológicas de la actualidad.

Otro punto importante aquí es que nos comentan sobre la responsabilidad del trabajador y su trabajo en equipo como factores que ayudan notablemente a la adquisición de conocimientos con bases fuertes, este conocimiento representa a futuro en una iniciativa porque permite adelantarse hacia procesos futuros que permitan potencializar el negocio de una manera amplia y con vista a la consecución de objetivos.

También existe otros puntos de vista en que se refiere a que no es necesaria una formación académica sino un conjunto de conocimientos básicos, pero que ayudados

por la experiencia que se toma día a día, resultan favorables al proceso por ejemplo de toma de decisiones, concuerdan en que la experiencia es el mejor modelo de adquisición de conocimientos, pero también existe un gran limitante porque aquí no hay un título que respalde dicha formación, y al final resulta un poco frustrante para aquellos que desean superarse por tanto si existe un lazo de la experiencia con la preparación resultaría la creación de líderes con una actitud formativa a la excelencia y al crecimiento profesional.

Pregunta 11. ¿Al realizar actualizaciones al sistema se realizan pruebas de control para verificar la estabilidad de dicha actualización?



Iniciando el análisis de la información podemos constatar que en un 47% de las firmas, utilizan pruebas de control para verificar la estabilidad de la actualización porque es importante para que en el futuro no existan diferencias en los datos ingresados y procesados así como también la presentación de informes resulte igual o mejor al realizar este tipo de mejora al sistema, en concreto para todas las empresas no existe una persona en específico para realizar esta certificación por lo tanto se encontró que algunos casos realizaba el departamento de sistemas, el área de tecnología, el analista de sistemas y también una persona que maneja el sistema de información en conjunto con la empresa que da el servicio de software.

También se pudo detectar que en pocos casos el sistema que utilizan no realiza actualización sino que la licencia que utilizan del software tiene el periodo de validez de un año y que cada año se tiene que comprar la nueva licencia y esta viene con los cambios y actualizaciones que se necesita.

Con respecto al 53% restante en realidad no realizan cambios y no actualizan al sistema porque depende de la infraestructura de la misma al ser organizaciones con poco personal y un sistema basado en hojas de cálculo pues hace que no se necesite realizar actualizaciones constantemente a los sistemas.

Pregunta 12. ¿Existe una política en la organización para instalar las actualizaciones de nuevas versiones?

Tabla 8.

Política para instalar actualizaciones.

SÍ	19	38,78%
NO	27	55,10%
No Contesta	3	6,12%
TOTAL	49	100,00%

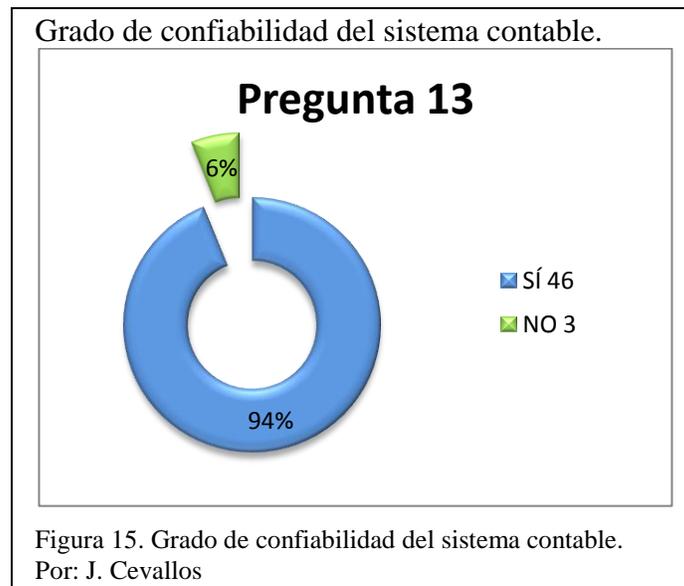
Nota: Empresas que tienen como política instalar actualizaciones

Iniciando el análisis de la información se encontró que en un 39% de las firmas tienen como política interna de la organización actualizar los sistemas porque depende mucho de la situación actual por las normativas que se presentan actualizar los componentes, también se encontró que algunas de las firmas se reunían constantemente con el departamento de sistemas en conjunto con un analista de la información para que en conjunto se tome la decisión de actualizar el sistema, otra opinión importante es que las firmas que tienen presencia internacional envían un correo electrónico sobre cambios en las políticas y en el sistema de tal forma que llegada cierta fecha las áreas que tenían actualización debían dejar el ordenador prendido para que automáticamente se realicen los cambios.

Con respecto al 55% restante no tiene una política interna en la organización para realizar actualización a los sistemas simplemente de acuerdo a la necesidad de la

empresa se realizan los cambios necesarios, por ultimo en lo que se refiere al 3% restante no contestaron esta pregunta.

Pregunta 13. ¿El sistema de información del área contable es confiable y seguro por lo tanto permite evaluar las competencias de los usuarios que la utilizan?



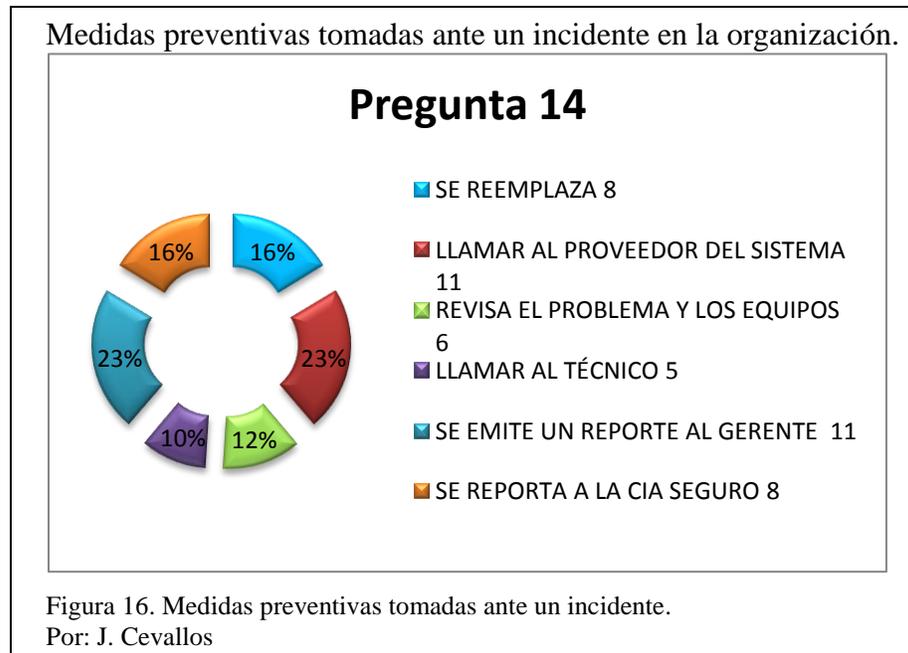
Se puede detectar con esta pregunta el porcentaje de eficiencia de la operación con un 94%, que en este caso permite obtener una seguridad completamente razonable sobre el sistema de información contable, por lo tanto es necesario describir algunas de las observaciones encontradas por ejemplo, que a través de esta plataforma se permite evaluar la competencia de trabajo en equipo al unir los datos de otras áreas y que permite obtener reportes rápido y en tiempo real.

También evalúa la capacitación del usuario ya que a través de una serie de indicadores le permite tomar de decisiones para la organización, evalúa también la responsabilidad del trabajo porque se maneja con información de terceros y estos a su vez con confidencialidad y con el debido cuidado que merecen, por ultimo manejan lo que es la orientación al servicio ya que a través de las decisiones se da asesoría al cliente sobre las posibles soluciones que debe tener en su negocio u organización.

En lo que respecta al 3% restante cabe recalcar que en este grupo están aquellos que no contestaron esta pregunta es decir 1 firma y de ellas 2 firmas no llevan la

contabilidad o la actividad financiera sino una empresa contratada para dicha actividad.

Pregunta 14. ¿Cuándo existe un problema de infraestructura es decir un daño o perdida de algún equipo las medidas preventivas y correctivas se toman en ese instante indique el procedimiento?

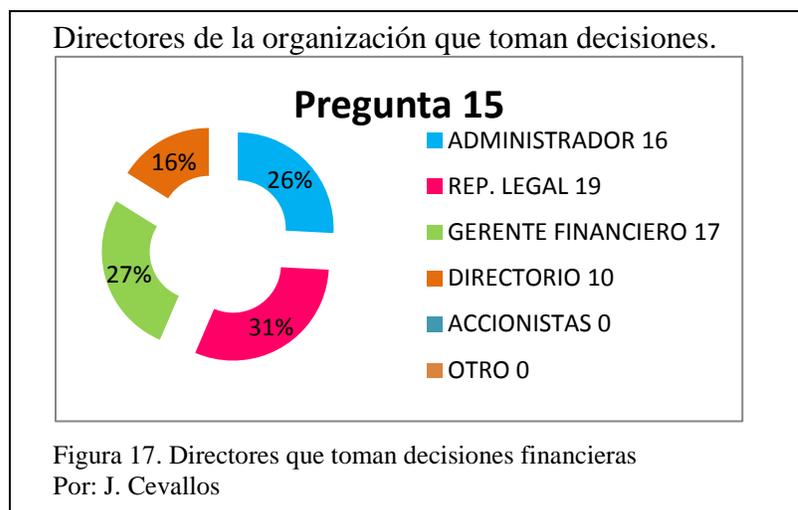


En esta pregunta encontramos respuestas muy variadas para empezar por las firmas que reemplazan el equipo inmediatamente después del siniestro pues le corresponde a un 16%, después tenemos con un 16% las organizaciones que llaman al proveedor del sistema para que cambien el equipo defectuoso y se proceda con el arreglo correspondiente, el 12% revisan el problema, los equipos y tratan de buscar por su cuenta una solución que sea favorable y evitar gastar recursos innecesarios.

El 10% de las firmas cuando sucede este tipo de inconvenientes llaman al técnico y verifican si es viable una reparación para aminorar los costos, caso contrario se procede con la compra de un nuevo equipo, tenemos también otro 23% que al momento de ocurrido el problema realice el reporte al gerente para que a su vez tome la decisión de llamar a un técnico para la reparación, hablar con el proveedor o tomar la decisión de reponer automáticamente el equipo.

Por último tenemos las firmas que reportan a las compañías de seguro con un 16% para que se proceda con la reposición de los equipos, cabe recalcar que la mayoría de estas empresas en su contrato en el que brindan asesoría y mantenimiento de equipos por tanto si solo necesitan la reparación la aseguradora brinda este servicio completamente gratis.

Pregunta 15. Cuando se deben tomar decisiones sobre presupuestos, inversión, capital los realiza:



Como se puede observar en la tabla y gráfico anterior se evidencia cada uno de los porcentajes de los representantes de cada compañía para tomar las decisiones financieras de la organización, en la siguiente tabla se muestra como se distribuyen cada uno de los representantes de las organizaciones de forma porcentual:

Tabla 9.
Distribución de forma porcentual de las decisiones tomadas.

DECISIÓN	CANTIDAD	%	DECISIÓN 1	% TIPO 1
1	39	79,59%	29	59,18%
2	7	14,29%	10	20,41%
3	3	6,12%		
3	49	100,00%		

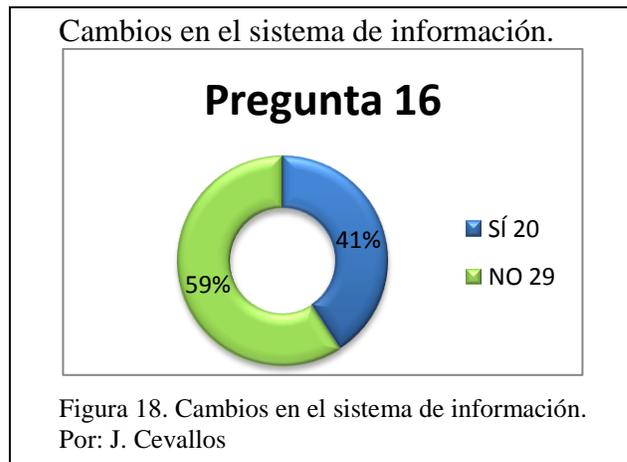
Nota: Distribución porcentual del tipo de decisión

Por lo tanto se puede observar que en el primer caso solo uno de los representantes de la información toma decisiones financieras con un 80%, ahora de este valor se le resta

el 20% es decir 10 compañías porque en estas las toma las decisiones el directorio únicamente, por tanto nos quedarían solamente 29 empresas en las que toma las decisiones un representante y su valor porcentual con respecto a las demás es del 60%.

Con respecto a las firmas en las que toman dos personas las decisiones en conjunto corresponde a un 14% en este caso mejora el riesgo de error ya que la responsabilidad es compartida para las dos personas, por ultimo tenemos con un 6% el grupo de firmas en que toman las decisiones el representante legal, el administrador y el gerente financiero por lo tanto la responsabilidad se comparte entre ellos y el riesgo de toma de decisiones es aún menor que en el anterior porcentaje.

Pregunta 16. ¿Se han realizado cambios últimamente en algún sistema de información que la organización tiene y a su vez a mejorado la productividad o la calidad de servicio?



Iniciando el análisis podemos identificar que el 41% de las firmas si ha realizado cambios en el sistema de información por tanto ha mejorado su productividad en materia económica, ha mejorado el valor agregado a sus servicios, la calidad de la información se maneja confiable y disponible para tomar decisiones así como también la implementación de nuevas estrategias organizacionales encaminadas a actualizar los sistemas y mantenerse a la vanguardia en conjunto con las leyes y normativas actuales.

En lo que respecta al 59% por diferencia nos dice que no se han realizado cambios en el sistema por lo tanto, no es necesario mejorar la productividad y la calidad de los servicios hacia los clientes ya que únicamente confían el sistema actual que les brinda una certeza razonable en base a las decisiones tomadas para mantener el negocio saludable y rentable.

Pregunta 17. ¿La actualización de conocimientos de los colaboradores o usuarios permite a la organización promover cargos cuando los conocimientos sean lo suficientemente amplios para poder aplicarlos?

Para la mayoría de las empresas resulta muy necesaria y útil la actualización de los conocimientos de los usuarios porque les permite desarrollar nuevas estrategias para mejorar el análisis de los datos y ofrecer a los clientes un servicio de calidad de tal forma que permite el incremento de la capacidad de la organización para tomar decisiones y por su mejora en los procesos en referencia al giro del negocio.

Otro punto importante es que una promoción de cargo conlleva un aumento de sueldo por lo tanto resulta como un incentivo para mejorar al colaborador, le permite tener una seguridad de que su conocimiento y experiencia es valorado por lo tanto su preparación hace que el desarrollo no sea solo para la empresa sino también para el usuario.

También podemos hablar de las competencias profesionales como trabajo en equipo, calidad de la información, mejora en tiempos de los procesos que permiten al usuario entregar nuevas ideas ya sean estas innovadoras que permitan refrescar la imagen, los procesos, el clima laboral, así como también de buscar el desarrollo de la responsabilidad social que deben tener todas las organizaciones encaminadas a mejorar o dar un apoyo a la sociedad en estratos donde la ayuda del gobierno no llega.

Pregunta 18. ¿Existe algún tipo de convenio con alguna empresa de seguridad para salvaguardar los activos físicos de la organización?



Como se puede evidenciar el 45% de las firmas auditoras tienen contratado con una compañía de seguridad el servicio de guardianía para resguardar los activos físicos de la organización, esto resulta de un gran beneficio y de una mejora en materia de seguridad porque salvaguarda uno de los activos más importantes para la organización, por lo otro lado también existe lo que es la vigilancia y la seguridad remota por lo tanto a través de cámaras y sistemas de seguridad con sensores de movimiento que se activan cuando existe intrusión o movimiento en las instalaciones de la organización.

Con respecto al 55% restante resultan dos motivos por los cuales las empresas no contratan un servicio de seguridad y se detalla así:

1. En primera instancia tenemos una alarma de seguridad pero la misma que a ser activada emite una señal a los servicios públicos de seguridad y al o los encargados de la seguridad de la organización a través de un mensaje de texto o llamada telefónica.
2. La segunda opción que se manejan en seguridad las firmas es que sus oficinas están ubicadas en edificios con seguridad privada por lo tanto el servicio de guardianía no solo cubre a la organización sino a todo el conjunto de oficinas que están actualmente ocupadas en el bien inmueble por lo tanto se paga por servicio compartido para todas las empresas del sector donde esta ubicada.

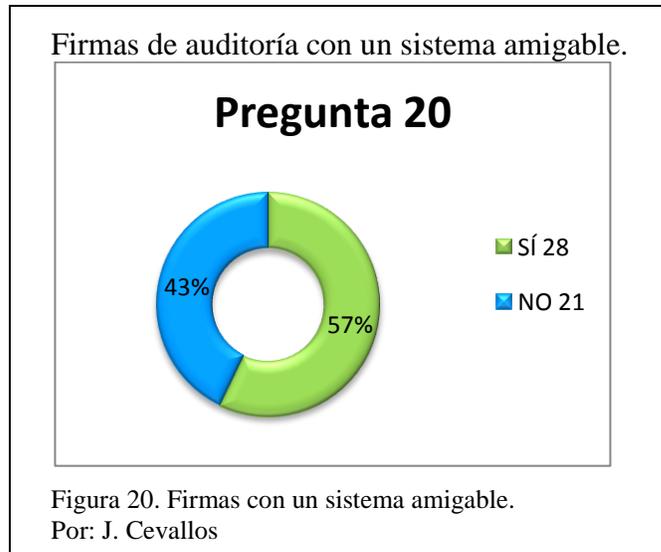
Pregunta 19. ¿Los reportes que se emiten en base a la información que emite el sistema están parametrizados para que solo los puedan analizar los administradores, directores o gerentes?

Partiendo de la premisa de seguridad tenemos que para revisar reportes se permite solo el ingreso a los logs solo usuarios con privilegios de administrador o con claves de seguridad y roles específicamente creados para estas actividades de esta manera se evita que usuarios no registrados en la red o sin permisos puedan acceder a este tipo de información que en realidad es sensible para todos los casos.

Por otro lado tenemos que la responsabilidad es compartida por lo tanto los reportes a si como la toma de decisiones las toma en conjunto el representante legal con administrador o el gerente se esta forma se mantiene la seguridad razonable y se baja en gran manera el riesgo por decisiones apresuradas y tomadas sin prestar atención a otros puntos de la organización que se complementan y que pueden llevar a una mejora sustancial de resultados.

Por último tenemos aunque en un pequeño número de firmas no emitir reportes esto ya que se manejan directamente con la información de los clientes, de esta manera se elimina la posibilidad de tomar de decisiones porque su trabajo se centraliza en la realización de informes para los clientes en base a sus datos por ende el giro de su negocio se concentra en el cumplimiento de las actividades inherentes y a la satisfacción del cliente externo.

Pregunta 20. ¿La interface del sistema permite una conexión amplia entre el usuario y el ordenador de tal forma que resulta fácil la interpretación y análisis de los datos?



En esta pregunta podemos encontrar con un 57% de firmas que utiliza su sistema es de fácil interpretación por lo tanto resulta amigable con el usuario, tiene algunas ventajas que permite la reducción de tiempo en la entrega de resultados y permite la posibilidad de encontrar soluciones en el instante que ocurren para mejorar los procesos productivos, estos sistemas ayudan al mejoramiento de la planeación y proyección de datos porque permiten la integración de mas sistemas en lugar de utilizarlos por separado, además permite la fácil capacitación al usuario que va a utilizar porque reduce el tiempo de entrenamiento.

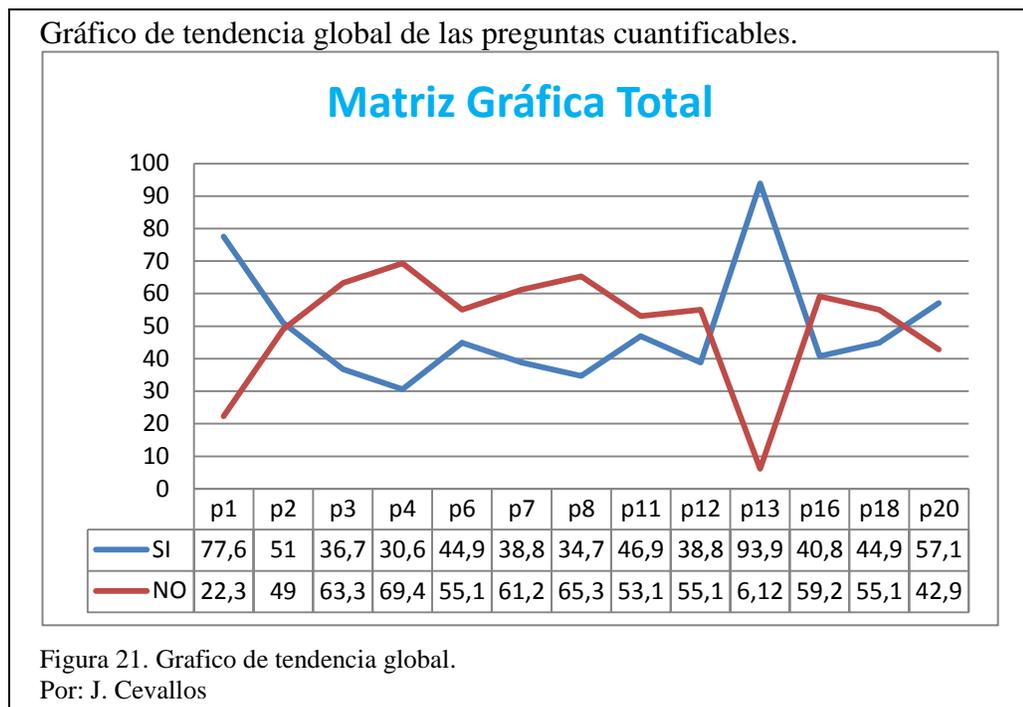
Existen firmas que tienen fácil la interpretación de datos porque tenemos el hecho de que permite la optimización de archivos es decir no se crean distintos tipos de formatos para cada aplicación sino que uno solo enlaza y permite la interconexión y fácil uso de la información y se emita los reportes a una sola base de datos requerida de esta forma se elimina la posibilidad de duplicación de información y estos aplicativos están hechos para que todos los usuarios sean capaces de manejar el sistema.

En lo respecta al 43% restante no es que el sistema no sea amigable sino que simplemente ofrece la información de nuestros procesos pero no en conjunto, no necesariamente en tiempo real, no emite informes relacionados a las demás áreas sino específicamente de cada una y se limita solo a la presentación de resultados sin la

posibilidad de ofrecer otras opciones con ventajas de tipo económico, tiempo o productivo.

4.2 Gráficos de tendencia

A continuación se presentan los siguientes gráficos con tendencia que se obtienen de cada una de las preguntas en las que se puede cuantificar su respuesta:



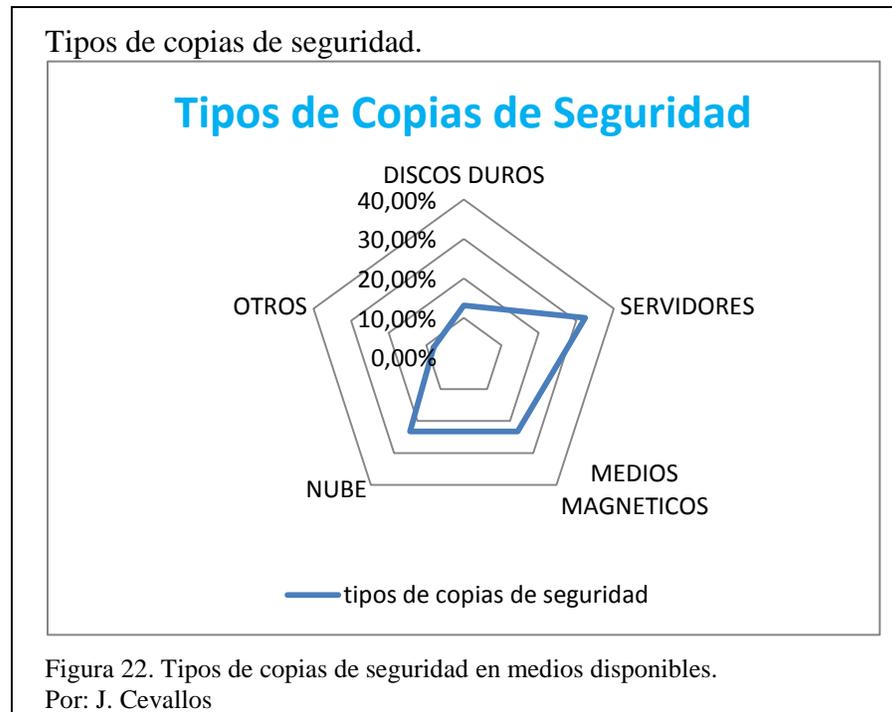
Pregunta 5. ¿Se entiende que deben existir copias de seguridad del sistema cuales son los medios disponibles?

Tabla 10.
Copias de seguridad en medios disponibles.

P5	Discos duros	13.13%
P5	Servidores	32.32%
P5	Medios magnéticos	23.23%
P5	Nube	23.23%
P5	Otros	8.08%

Nota: Medios disponibles para copias de seguridad.

Realizando un gráfico de tendencia podemos mirar a que tipo de copia de seguridad se inclina más de esta forma tenemos:



Pregunta 14. ¿Cuándo existe un problema de infraestructura es decir un daño o perdida de algún equipo las medidas preventivas y correctivas se toman en ese instante indique el procedimiento?

Tabla 11.

Tipos de medidas preventivas ante un incidente.

P14	Se reemplaza	16.33%
P14	Llamar al proveedor del sistema	22.45%
P14	Revisa el problema y los equipos	12.24%
P14	Llamar al técnico	10.20%
P14	Reporte al gerente	22.45%
P14	Se reporta a compañía de seguro	16.33%

Nota: Medidas preventivas ante un incidente.

Realizando un análisis gráfico tenemos en un porcentaje similar la tendencia tiende a dirigirse al reporte al gerente y al proveedor del sistema, es decir que estas medidas preventiva tienen un porcentaje de aceptación superior entre las firmas.



Pregunta 15. Cuándo se deben tomar decisiones sobre presupuestos, inversión, capital los realiza:

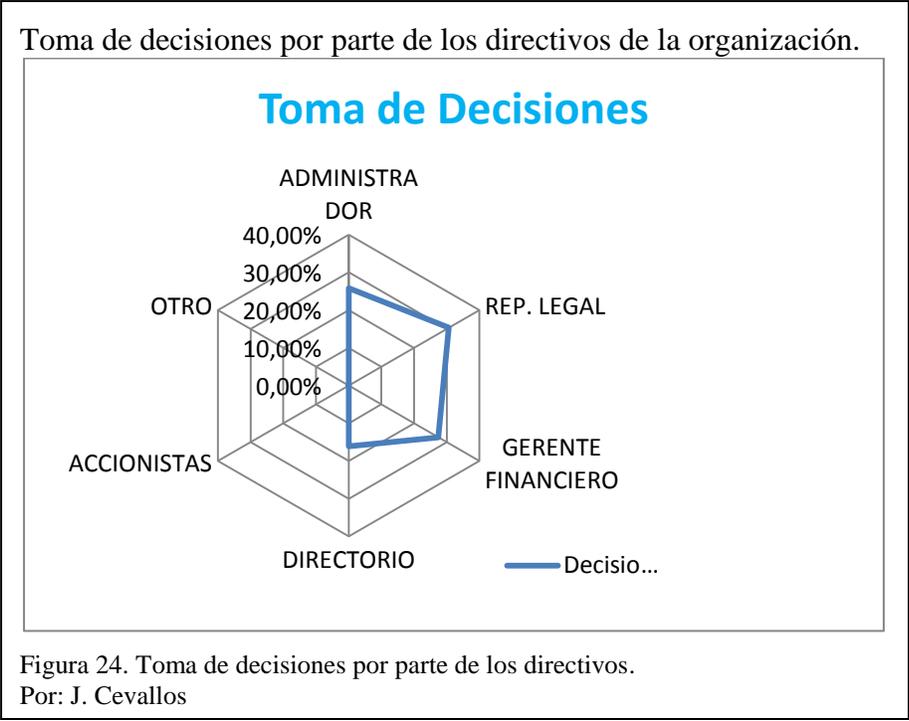
Tabla 12.

Tipos de directores que toman las decisiones.

P15	Administrador	25,81%
P15	Rep. Legal	30,65%
P15	Gerente financiero	27,42%
P15	Directorio	16,13%
P15	Accionistas	0,00%
P15	Otro	0,00%

Nota: Decisiones de los directores en porcentaje.

En la siguiente figura se tiene como muestra la tendencia al aplicar las decisiones en las firmas por parte de los directivos.



4.3 Informe de resultados

A través de la encuesta realizada a las firmas auditoras del cantón Quito se logró determinar la siguiente información con el fin de dar a conocer sobre los puntos de interés más importantes de acuerdo a sus procedimientos y políticas para la gestión de la información así:

En el área de usuarios destacamos el hecho de que en un porcentaje mayor al 70% de las firmas utiliza cuentas de usuario para mejorar la seguridad al momento de ingresar a un ordenador, también se destaca el hecho que existe software del sistema que cuenta con perfiles de acceso que limita el uso de los usuarios y que por lo tanto da una segunda opción de control y seguridad en un 51% de las organizaciones encuestadas, el uso de claves en red se limita solo a un 37% de las entidades por tanto resulta de más riesgo para la gestión de los datos que van a ser utilizados debido a la modificaciones que se pueden dar. Por último tenemos el control de la actividad de los usuarios para evitar que ingresen a sitios restringidos por la organización o acceder a contenido diferente al que está asignado analizando en porcentajes tenemos que solo un 31 de las firmas mantiene este control hacia los colaboradores.

En lo que se refiere al área de seguridad se detallo cuatro opciones de seguridad pero también existía la opción de detallar otras opciones para backups de la información de tal forma que se encontró lo siguiente. discos duros 13%, servidores 32%, medios magnéticos 23%, la nube 23%, y otras opciones tenemos un 8% como dropbox, box, icloud, Onedrive adicional a esta información tenemos en conjunto con los datos anteriores que el 22.45% de las firmas utilizan solo uno de los medios antes mencionados, el 53.06% utiliza dos tipos de medios de almacenamiento y el 24,49% utiliza tres medios de seguridad para realizar backups de su información, además tenemos un margen de seguridad del 45% que en realidad es bajo para mantener los archivos disponibles a todos los usuarios que utilizan los datos de la organización.

En el área de infraestructura identificamos que el 39% de las firmas aseguran sus equipos y el software ante cualquier eventualidad que puedan tener lo que nos indica que el porcentaje restante no los tiene asegurado por lo tanto se debe aplicar medidas correctivas para mitigar este riesgo en las organizaciones, ahora si nos enfocamos en las políticas de las organizaciones el 65% no tiene un manual de procedimientos en que el indique el uso correcto de los equipos para su mantenimiento adecuado así como también las sanciones que debe existir cuando no se tiene cuidado al manejar los equipos de la organización.

En lo que se refiere a las capacitaciones se determino en un porcentaje menor o igual al 10% de las firmas no capacitan a los usuarios cuando se realizan cambios en el sistema porque utilizan aplicativos que no tienen mayor complejidad y cuando se realizan dichos cambios no se necesita de una capacitación especial para estas modificaciones, otra opción utilizan hojas de cálculo para sus procesos por tanto no se requiere de modificaciones o capacitaciones, por ultimo tenemos que en las entidades pequeñas muchas de las veces solo se cambia o se modifica la información de aquellos usuarios que lo necesiten de acuerdo a las necesidades de la empresa.

También se encontró la información referente a la formación académica como un factor importante en el desempeño de actividades y en su mayoría de organizaciones concuerda que se debe dar prioridad en la capacitación profesional de los usuarios de esta forma se logra procesos eficientes y con miras a cumplir los objetivos de la organización, en menor tiempo posible y el menor uso de recursos convirtiéndolas en entidades más rentables.

Las actualizaciones del sistema mediante pruebas de control antes de su implantación tiene un 46.94% de aceptación en las firmas para probar la estabilidad de las misma y que por lo general lo realiza el departamento de sistemas o tecnología de la información, a continuación tenemos que en un 38,78% de las firmas tiene como política actualizaciones de nuevas versiones para su software esto con el fin de mejorar la confiabilidad del sistema hacia sus usuarios.

En el área de toma de decisiones se encontró que en un 93,88% de las firmas su aplicación para la gestión de la información contable permite evaluar las competencias de los usuarios que lo utilizan en sus diferentes indicadores como son la confidencialidad, el trabajo en equipo, el cumplimiento de obligaciones referentes al uso de información de terceros.

En el estudio de las medidas correctivas para mitigar incidentes hacia los equipos tenemos que en un 16,33% reemplaza el equipo, el 22,45% llama al proveedor del sistema e informa de la situación, el 12,24% revisa el problema por su cuenta, el 10% llama al técnico para que revise y arregle el problema, el 22,45% emite un reporte al gerente y por último el 16,33% reporta el caso a la compañía de seguro para el mantenimiento o restitución del equipo.

Con respecto a las decisiones que se deben tomar para presupuestos inversión y capital se determino que el 25,81% lo realiza el administrador, el 30,65% lo realiza el representante legal, el 27,42% los realiza el gerente financiero y un 16,13% el directorio y en conjunto esta información se determino que en un 60% solo una persona toma las decisiones, un 14% las toman entre dos de los representantes y solo el 6% comparten tres personas su información para la toma de decisiones.

El 41% de las firmas ha realizado cambios en sus sistemas de información de tal forma que se ha logrado en una mejora en los tipos de servicio que ofrecen a sus clientes así como también en las recomendaciones que realizan a ellos sobre el giro de su negocio, en este punto también se destaca la actualización de conocimientos de los colaboradores para promoción de cargos es decir que con un nivel amplio de conocimientos seguido también de la experiencia resulta de un gran beneficio para poder alcanzar desarrollo profesional.

Con respecto a la seguridad de los activos de la organización se determinó que en un 44,90% de las firmas tiene contratado un convenio con una compañía de seguridad para salvaguardar sus activos, el 55,10 restante no tiene convenios porque cuentan con alarmas de seguridad conectadas con servicios de seguridad pública y también

porque se encuentran ubicadas sus oficinas en instalaciones con seguridad de terceros.

En lo que se refiere a los reportes para los administradores o directores estos se encuentran parametrizados para que de acuerdo a su nivel jerárquico solo ellos puedan revisarlos y tomar las decisiones que correspondan a cada caso, solo existe un pequeño número de firmas que no emite reportes y la razón es porque trabajan con información de terceros y no resulta necesario.

Revisando el tema de la interface se encontró que un 57,14% de las firmas tiene un sistema amigable de fácil interpretación y que por tal motivo resulta conveniente al momento de tomar decisiones para que ellos usuarios que lo pueden realizar y el 42,86% restante pues no significa que tiene un sistema adecuado a su organización sino que esta dimensionado para que se integre por partes y solo ofrece la posibilidad de realizar opciones operativas mas no el fin del incremento de su productividad.

Por lo tanto los hechos descritos anteriormente resultan de la investigación realizada para obtener el mayor número de datos posibles y poder emitir las conclusiones y recomendaciones respectivas.

JAC

Realizado por. Juan Cevallos Rubio

CONCLUSIONES

1. La apertura de las firmas de auditoría del cantón Quito ha sido considerable para poder realizar el presente trabajo de investigación así pues, se logro desarrollar este proceso de una forma organizada con un conjunto de procedimientos lógicos y con una metodología aplicada a los plazos establecidos, de tal forma que se nos permitió el uso y el análisis de los datos referente a los sistemas de información que poseen las empresas auditoras para posteriormente detectar aquellas debilidades que afectan el buen manejo y gestión de la información de ahí el interés de proponer medidas de acción correctivas para la solución de problemas.
2. Un aspecto a considerarse es la seguridad de la información se debe estar consciente de los cambios globales en las organizaciones en materia de seguridad ya que no solo es importante una clave o una cerradura que impida la substracción de la información se debe entender este tema como una necesidad mundial un recurso digital que permite la optimización de recursos financieros, materiales, tecnológicos de tal forma que es imprescindible la actualización y entrenamiento sobre el proceso de resguardo de la información.
3. Un punto a destacar es la importancia de tener un plan de contingencia que involucre a todo el personal los equipos de la organización, el software y las aplicaciones informáticas con el fin de establecer los controles necesarios para salvaguardar la información con el fin de garantizar la integridad y la confidencialidad de los datos ante cualquier siniestro que pueda ocurrir, este plan debe contener las directrices para el análisis de los posibles riesgos a los que esta expuestos el (hardware y software) y toda la información contenida en estos medios por lo tanto el plan de contingencia permitirá identificar los riesgos antes durante y después de haber ocurrido para su posterior control.
4. En la actualidad existen un conjunto de normas ISO que permiten la organización de los datos de una manera segura, establece como se debe

implantar este conjunto de políticas dentro una organización de tal forma que esté disponible y sea accesible a todos los miembros de las entidades, también establece como una media de seguridad el control que se le debe dar a los usuarios al darles el nivel de acceso que cada uno de ellos necesita por ultimo tenemos los controles que se debe dar al hardware y software de la organización como un recurso indispensable y necesario para la toma de decisiones.

5. Se destaca el aspecto teórico de esta investigación porque existe una gran disponibilidad de recursos disponibles para analistas programadores y técnicos que desean conocer los aspectos más significativos para la aplicación de sistemas orientados al mejoramiento de soluciones empresariales basados en una seguridad efectiva de la información, también se destaca todos los datos disponibles para aquellos emprendedores directores y administradores sobre el tratamiento de la información en base a la seguridad, infraestructura, uso de medios para la realización de copias de seguridad, medidas técnicas para la implantación de sistemas y que estas estén adecuadas al entorno de la organización.
6. Existe una gran predisposición de la empresas para mantener cuentas de usuario como primer filtro para el ingreso al sistema general, pero por el contrario sube mas el riesgo por perfiles de acceso porque existe menos firmas que utilizan este recurso como medida seguridad para sus aplicaciones principales, las mismas que deben tener la opción de realizar copias de seguridad en el mayor numero de medios disponibles y así evitar el riesgo de pérdida de la información.
7. Los manuales y reglamentos son importantes al momento de delimitar el uso de equipos y sistemas y lo es aun mas cuando existe un procedimiento en el que indica que se debe contratar una póliza de seguro para mantener a los equipos resguardados ante cualquier eventualidad que se suscite en la organización.

8. La capacitación la experiencia y la orientación al servicio de las organizaciones desempeñan un papel fundamental para aquellos directivos que desean tomar decisiones que beneficien al buen desempeño de la actividad comercial y alcance de resultados esto en unión a una plataforma amigable y que permita la integración fácil de los datos alimentados por todos usuarios dan la oportunidad de presentar de reportes en tiempo real y disponibles para poder ejecutar medidas de prevención de ser el caso y otras con vista al desarrollo del proceso organizacional y comercial de las firmas.

9. El sistema de información en conjunto con el hardware y los usuarios debe coexistir de una forma equilibrada, amigable y confiable de esta manera se garantiza el acceso a los datos en tiempo real, permita tener un control a los usuarios su acceso sus permisos, también debe permitir emisión de reportes basados en hechos y datos ingresados en las bases de datos por los usuarios de una manera responsable y apegada a las políticas y normas de la institución de esta forma se garantiza la calidad de la información y de los procedimientos aplicados a la misma, en conclusión la adopción de normas ISO que permiten garantizar la seguridad de todos los elementos que conforman el sistema de información y su tratamiento esto, lógicamente para organización que poseen la infraestructura, el recurso humano, tecnología y capacidad financiera que permita solventar esta inversión, para aquellas empresas que no tienen los recursos necesarios pues únicamente revisar toda la información concerniente a las normas y adaptarlas a su entorno organizacional, por la tanto la toma de decisiones se basaran en datos coherentes y con miras a cumplir con todos los objetivos planteados por la organización.

RECOMENDACIONES

1. Se recomienda realizar periódicamente un control al sistema de información de tal forma que se puedan determinar cambios a manuales, políticas y procedimientos existentes pero también añadir la adopción de nuevas tecnologías y nuevas formas para el tratamiento y gestión de la información.
2. Es recomendable la utilización de cuentas de usuario y la opción de registro en red en primera instancia porque resulta del primer bloqueo para evitar la intrusión de usuarios no registrados en la red, como segundo procedimiento adoptar la medida y creación de perfiles de usuario a las aplicaciones es decir, que cada persona que utilice un programa se encuentre habilitado para una sola tarea en específico de esa aplicación porque puede ser que varios usuarios utilicen el programa de esta manera se limitan los roles de cada persona.
3. Para los backups de la información es indispensable el uso de tres medios para el resguardo de la información, esto debido al alto índice de hackeo de cuentas de usuarios, de recursos de red, pérdida o mala manipulación de los datos, substracción, deterioro del hardware en el que está asilado, debido a esto también es conveniente que los archivos de la organización referentes a datos sensibles no estén disponibles para todos los usuarios sino solo para aquellos que necesitan tomar decisiones o evaluar los datos obtenidos.
4. Es indispensable asegurar los equipos de la organización ya que este es el elemento principal de las actividades tenemos que en un 60% aproximadamente no lo hace por tanto tener un seguro representa estar un paso adelante ante cualquier situación que se pueda suscitar en la entidad, en un porcentaje igual se concentra lo que es el manual para un adecuado uso de los equipos que es imprescindible ya que sin esta normativa no podemos controlar el activo que representa importante para la empresa y para el usuario que utiliza.

5. En lo referente a posibilidad de que exista una política para la instalación de nuevas versiones es sumamente necesaria por seguridad y estabilidad del sistema, en un 60% aproximadamente no tienen esta norma en sus organizaciones representa un riesgo un alto porque de acuerdo a los datos obtenidos el 53.06% no realizan pruebas de control a las actualizaciones que se implantan por lo tanto en promedio del 50% no se tiene un control de aquellas modificaciones que se realiza a las aplicaciones.

6. En lo referente a la toma de decisiones es conveniente que los administradores, representante legal y el gerente financiero tomen las decisiones en conjunto porque eso mitiga el riesgo de cometer errores financieros en el área de inversión presupuesto y capital de esta forma se da una continuidad saludable a la organización en base a decisiones acertadas para su bienestar.

7. Es recomendable que en más de un 40% de las organizaciones cambien actualicen o modifiquen su sistema de tal forma que se pueda compartir información de manera mutua con las demás áreas o usuarios y eliminar la consolidación de reportes por parte del usuario sino que el sistema facilite este proceso de esta manera se emitirán los reportes a la dirección para que se tomen las decisiones en base a datos oportunos, confiables y que permiten planificar a futuro proyecciones y situaciones para el mejoramiento y bienestar de la organización y además que permitan inclusive para los organismos de control verificar toda la información contenida en la entidad sin ningún problema.

LISTA DE REFERENCIAS

- Acissi. (2013). *Seguridad Informática Ethical Hacking*. Conocer el ataque para una mejor defensa. Ediciones Eni.
- Acronis. (2014). *Gestión de copia de seguridad y almacenamiento para empresas*. Recuperado el 28 de Julio de 2014, de <http://www.acronis.com/es-es/company/>
- Aguilera López, P. (2010). *Seguridad Informática*. Madrid: Editex.
- Amaya, A. J. (2009). *Sistemas de Información Gerenciales- Hardware, Software, Redes, Internet, Diseño*. Bogotá: Ecoe.
- Areitio, J. (2008). *Seguridad de la Información*. Madrid: Paraninfo.
- Cardozo Cuenca, H. (2006). *Auditoría del sector solidario*. México: Ecoe Ediciones.
- Chiavenato, I. (2006). *Introducción a la teoría general de la Administración*. Mc Graw-Hill. México: Mc Graw-Hill Interamericana de Editores S.A. de C.V.
- Corletti Estrada, A. (2011). *Seguridad por Niveles*. Madrid: Darfe Learning Consulting S.L.
- De Pablos, C., Lopez Hermoso, J. J., Martin Romo, S., & Sonia, M. (2004). *Informática y Comunicaciones en la empresa*. Madrid: Esic.
- De Pablos Carmen, J. J.-R. (2011). *Organización y Transformación de los Sistemas de Información en la Empresa*. Madrid: Gráficas Dehon.
- De Pablos, H. C., López, H. J., & Santiago Martin-Romo, S. M. (2006). *Dirección y Gestión de los Sistemas de Información de la Empresa*. Madrid: Esic Editorial.
- Deloitte Touche Tohmatsu Limited. (2013). *Los IFRS en su bolsillo*. Recuperado el 2014 de Mayo de 25, de <https://www.deloitte.com>.
- Díaz, G., Mur, F., Sancristobal, E., Castro, M.-A., & Peire, J. (2012). *Seguridades en las comunicaciones y en la información*. Madrid: Universidad Nacional de educación a Distancia.
- Echenique García, J. A. (2004). *Auditoría en informática*. México: Mc Graw-Hill S.A. de C.V.
- Fernández, A. V. (2006). *Desarrollo de Sistemas de Información Una metodología basada en el modelado*. Barcelona: UPC.
- García-Cervigón Hurtado, A., & Alegre Ramos, M. d. (2011). *Seguridad Informática*. Madrid: Paraninfo, SA.

- Giner de la Fuente, F. (2004). *Los Sistemas de Información en la Sociedad del Conocimiento*. Madrid: Esic.
- Gómez, M. M. (2006). *Introducción a la metodología de la investigación científica*. Córdoba - Argentina: Editorial Brujas.
- Grande Esteban, I., & Abascal Fernández, E. (2009). *Fundamentos y técnicas de investigación comercial*. Madrid: ESIC.
- Haizer, J., & Mender, B. (2008). *Dirección de la Producción y de las Operaciones - Decisiones Tácticas*. Madrid: Pearson Educación, S.A.
- Heinemann, K. (2003). *Introducción a la Metodología de la Investigación Empírica*. Barcelona: Editorial Paidotribo.
- Hellriegel, D., Jackson, S. E., & Slocum, J. W. (2009). *Administración Un enfoque basado en competencias*. México DF: Cengage Learning Editores, S.A.
- Hurtado León, I., & Toro Garrido, J. (2007). *Paradigmas y métodos de investigación en tiempos de cambios*. Caracas: Cec. S.A.
- IAASB, C. D. (15 de Diciembre de 2009). *Normas Internacionales de Auditoría*. Londres, Reino Unido.
- IWI, G. (2009). *Implantación de LOPD en las empresas medidas de seguridad*. Málaga: Vértice S.L.
- Laudon, K. C. (2008). *Sistemas de Información Gerencial*. México: Pearson Educación de México, S.A de C.V.
- Luna, Y. B. (2003). *Normas y Procedimientos de la Auditoría Integral*. Bogotá: Ecoe Ediciones.
- Maciá Pérez, F., Mora Gimeno, F. J., Gil Martínez-Abarca, J. A., Gilart Iglesias, V., Jorquera, D. M., Berná Martínez, J. V., y otros. (2008). *Administración de Servicios de Internet De la Teoría a la Práctica*. Murcia: Compobell, S.l.
- Madrigal Torres, B. E. (2009). *Habilidades directivas*. México DF: Mc Graw-Hill interamericana Editores, S.A. de C.V.
- Mantilla, S. A., & Cante S., S. Y. (2005). *Auditoría de Control Interno*. Bogotá: Ecoe Ediciones.
- Mesén Figueroa, V. (2007). *Aplicaciones Prácticas de las Normas Internacionales de Información Financiera*. Costa Rica: Editorial Tecnológica de Costa Rica.
- Mira Navarro, J. C. (2006). *Apuntes de Auditoría*. España.

Nanosystems S.r.l. (2014). *Software completo para la transferencia y copia de datos*. Recuperado el 28 de Julio del 2014, de <http://www.uranium-backup.com/es/uranium-backup-free/>

Paucar, N. (17 de Mayo de 2013). *Antecedentes de la Auditoría*. Recuperado el 16 de Mayo de 2014, de <http://consultadeber.blogspot.com/2013/05/antecedentes-clasificacion-y-tipos.html>

Pons Capote, O., Marín, N., Medina, R. J., Acid, C. S., & Vila, M. M. (2009). *Introducción a las bases de datos el modelo relacional*. Madrid: Paraninfo S.A.

Qbe Seguros Colonial. (2014). *Pólizas de seguro para equipo electrónico*. Recuperado el 28 de Julio de 2014, de <http://www.qbe.com.ec/formularios/>

Render, B., Hanna, M. E., & Stair, R. M. (2006). *Métodos cuantitativos para los negocios*. México: Pearson Educación.

Sampieri, R. H. (2006). *Metodología de la Investigación* Cuarta Edición. México DF: Mc Graw-Hill/ Interamericana Editores S.A de C.V.

Sánchez Guriel, G. (2006). *Auditoría a los Estados Financieros Practica Moderna Integral*. México: Pearson Educación de México S.A. de C.V.

Santos, D. d. (2007). *Toma de Decisiones Eficaces*. Madrid: Díaz de Santos S.A.

Soy I Aumatell, C. (2013). *Auditoría de la información identificar y explotar la información de las organizaciones*. Barcelona: Editorial UOC.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes Aplicaciones y Estándares*. Madrid: Pearson Education Inc.

Symantec. (2014). *Eficaz solución de creación de imágenes para PC y administración del ciclo de vida del equipo*. Recuperado el 28 de Julio de 2014, de http://www.symantec-norton.com/Norton_Ghost_15.0_p115.aspx?lang=es-EC