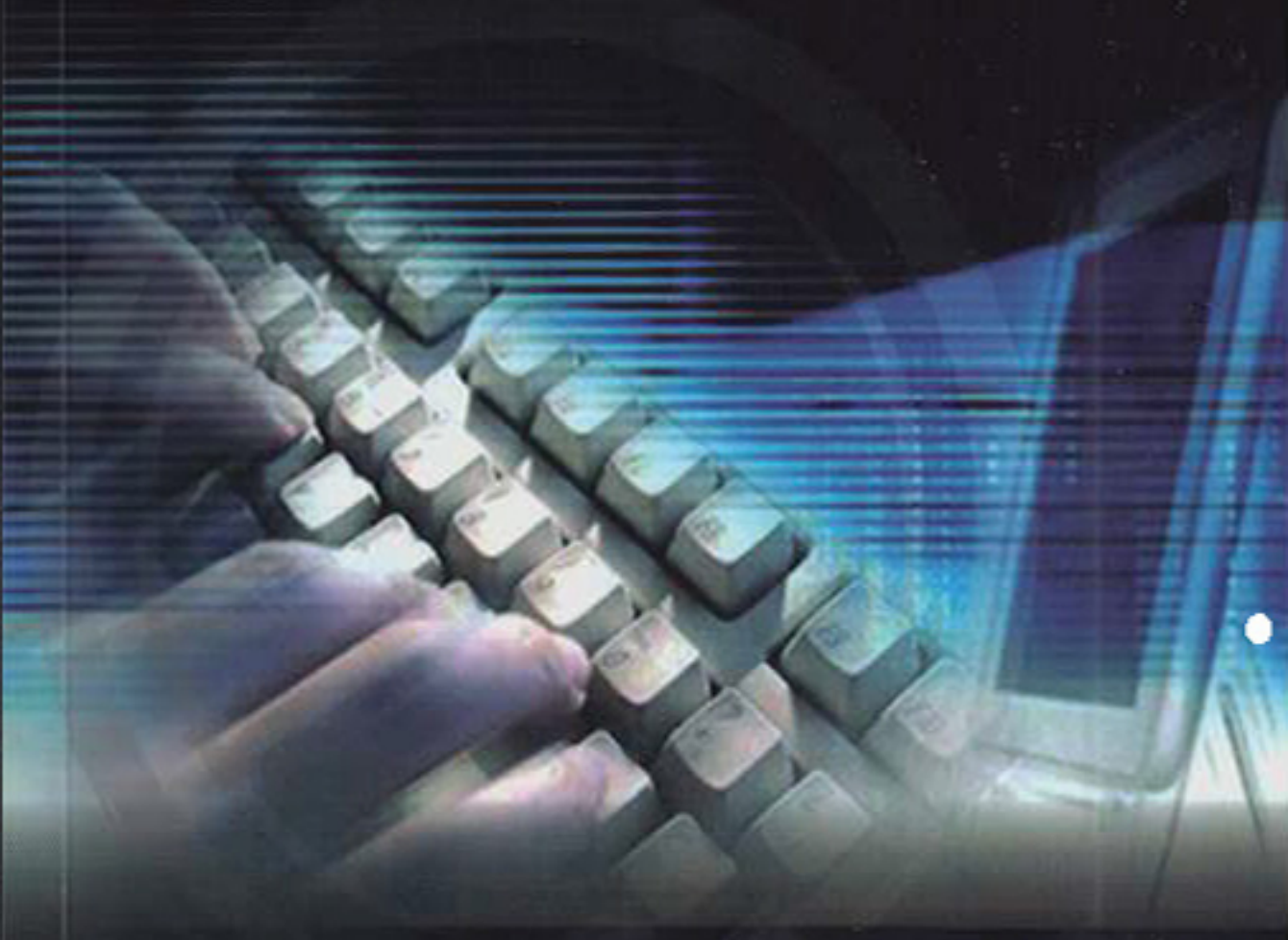
Libro de Investigación

Manual de Procedimientos para llevar a la Práctica la Auditoría Informática



FRANCISCO NICOLÁS JAVIER SOLARTE SOLARTE
ENITH ENILSE GUSTIN LÓPEZ
RICARDO JAVIER HERNÁNDEZ REVELO

Universidad Nacional
Abierta y a Distancia

Francisco Nicolás Javier Solarte Solarte
Magister en Docencia
Especialista en Auditoría de Sistemas
Especialista en Multimedia Educativa
Ingeniero de Sistemas
Docente de la Universidad Nacional Abierta y a Distancia UNAD

Enith Enilce Gustin
Especialista en Auditoría de Sistemas
Ingeniera de Sistemas
Coordinadora de Sistemas de la Institución Universitaria CESMAG

Ricardo Javier Hernández Revelo
Especialista en Multimedia Educativa
Licenciado en Matemáticas y Física
Tecnólogo en Sistemas
Docente de la IU CESMAG

MANUAL DE PROCEDIMIENTOS PARA LLEVAR A LA PRÁCTICA LA AUDITORÍA INFORMÁTICA

FRANCISCO NICOLÁS JAVIER SOLARTE SOLARTE
ENITH ENILSE GUSTIN LÓPEZ
RICARDO JAVIER HERNÁNDEZ REVELO

GRUPOS DE INVESTIGACIÓN FRANCISCO BELLINA BENCIVINNI
INSTITUCIÓN UwNIVERSITARIA CESMAG

GRUPO DE INVESTIGACION EN INGENIERIA Y EDUCACIÓN (GRIEE) UNAD

Solarte Solarte, Francisco Nicolás Javier, 2012

Manual de procedimiento para llevar a la práctica la auditoría informática / Francisco Nicolás Javier Solarte Solarte, Enith Enilse Gustín López, Ricardo Javier Hernández Revelo – 1ª ed. – San Juan de Pasto. Editorial Institución Universitaria Centro de Estudios Superiores María Goretti, 2012.

163 P. ilustraciones; 23 cm
Incluye referencias Bibliográficas (p. (161)-162)
Contiene Índice General

ISBN: 978-958-8439-25-9

1. AUDITORÍA DE SISTEMAS INFORMÁTICOS.
2. AUDITORÍA -- INNOVACIONES TECNOLÓGICAS.

CDD 657.450285

Catalogación en la publicación – Editorial Institución Universitaria Centro de Estudios Superiores María Goretti. Institución Universitaria CESMAG. Biblioteca Remigio Fiore Fortezza.

© Institución Universitaria CESMAG
Carrera 20ª 14-54
52002
Tel: +572 – 7216532 ext: 280 – 201
E-mail: goretti@iucesmag.edu.co
Website: www.iucesmag.edu.co
San Juan de Pasto, Nariño, Colombia

© Editorial Institución Universitaria Centro de Estudios Superiores María Goretti
Carrera 20ª 14-54
52002
Tel: +572 – 7216532 ext: 221 – 218 – 332
E-mail: editorial@iucesmag.edu.co
Website: www.iucesmag.edu.co/editorial
San Juan de Pasto, Nariño, Colombia

ISBN: 978-958-8439-25-9

A mi esposa Dey, a mis hermanos, a mis compañeros y amigos,
A la Universidad Nacional Abierta y a Distancia – UNAD
Y a todos los que han depositado la confianza en mí.

Francisco

Diseño de cubierta: Esp. Diseñadora Gráfica Erica Nathalia Mera Romo
Edición: Editorial Institución Universitaria Centro de Estudios Superiores María Goretti.
Diagramación: Esp. Diseñadora Gráfica Erica Nathalia Mera Romo
Impresión: TecnoGrafic - Pasto

Printed and made in Colombia

El pensamiento que se expresa en esta obra es responsabilidad exclusiva del autor y no compromete la ideología de la Institución Universitaria CESMAG.

A Dios por darme esta oportunidad,
a la Institución por permitirme participar en este proyecto,
a la Vicerrectoría de Investigaciones por su apoyo,
a mis hijos por su comprensión.

Enith

A DIOS, que nos permite llevar a cabo todos los proyectos de nuestra vida. A mi madre, padre y mis hermanos que han sabido tener la paciencia para acompañarme en los buenos y malos momentos, y a todos las personas que han sabido esperar y confiar en mi.

Ricardo

Agradecimientos

A la Institucione Universitaria CESMAG y a la Universidad Nacional Abierta y a Distancia - UNAD por su apoyo y colaboración en la realización de la investigación.

A todos los Ingenieros que participaron en la investigación con la información y sus aportes y contribuciones fundamentadas en la experiencia sobre el tema

Al Ingeniero Manuel Bolaños, por sus aportes en la revisión técnica y didáctica del documento que contribuyó con sus aportes y su conocimiento prestado a disposición de los autores.

A todos y a cada uno de los que participó en la elaboración de la investigación y los resultados plasmados en el presente manual de procedimientos.

Por último dar gracias a todos los autores e investigadores que son la fuente de inspiración para poder llevar a cabo esta obra.

CONTENIDO

INTRODUCCIÓN

Si continúas haciendo siempre lo mismo,
obtendrás siempre los mismos resultados.
Para conseguir algo nuevo, debes hacer algo diferente.
(Albert Einstein)

El manual que se presenta a continuación es el resultado de la investigación sobre las prácticas de los auditores de sistemas de la región y los problemas más frecuentes que se presentan de manera reiterada en las organizaciones empresariales de la ciudad de San Juan de Pasto, todo ello con el fin de determinar los objetivos de control de la auditoría y los procedimientos para llevar este proceso.

El manual se sustenta en la aplicación del estándar COBIT (Control Objective for Information Technology) que es la guía de mejores prácticas para el uso de la Tecnología en la gestión de procesos de Información; además el manual incluye los resultados obtenidos en distintos procesos de auditoría llevados a cabo bajo la dirección de los autores en varias organizaciones, la experiencia acumulada por los investigadores en esta área del conocimiento y fuentes bibliográficas existentes sobre el tema.

El manual pretende responder a las diferentes circunstancias y problemas de las organizaciones empresariales en el área informática en cuanto al uso de los recursos de tecnología y de los sistemas de información dentro de ella. Esta guía de procedimientos toma importancia por los altos costos que este proceso de auditoría involucra para la organización empresarial, ya que son pocos los ingenieros de sistemas que tienen el conocimiento en la aplicación de la auditoria informática y de sistemas.

El desarrollo de este estudio se sustenta en un conjunto de normas y estándares para realizar la auditoria informática y de sistemas, las metodologías y procedimientos para análisis de riesgos informático, la observación directa del manejo y administración de los recursos informáticos en organizaciones, los diferentes trabajos de grado de estudiantes de Ingeniería de Sistemas y especialización en Auditoria de Sistemas de las Universidades: Institución Universitaria CESMAG, Universidad de Nariño, UNAD y Universidad Antonio Nariño, además de la bibliografía existente sobre el tema.

El estudio responde a las diferentes circunstancias y problemas de las organizaciones empresariales en el área informática en cuanto al uso de los recursos informáticos y el uso de los sistemas de información dentro de ella. La investigación toma importancia por los altos costos que este proceso involucra para la empresa, por el poco conocimiento en la aplicación de la auditoria informática y de sistemas los ingenieros encargados de esta área no aplican estos procesos.

Se pretende mostrar, de manera didáctica, una guía para realizar procesos de auditoría informática y de sistemas, que pueda ser aplicada por los ingenieros de sistemas y personal de las empresas, contribuyendo así a disminuir costos que implica adelantar estos procesos, y contribuyendo a la formación de los profesionales en sistemas para que de manera fácil se adelanten procesos tendientes a detectar vulnerabilidades, identificar y evaluar riesgos, y solucionar problemas, o fallas que puedan afectar la funcionalidad del área informática y los sistemas software existentes en las organizaciones.

Los ejes temáticos que aborda el manual están relacionados con los fundamentos conceptuales de la auditoria informática y de sistemas, la metodología didáctica planteada a través de un ejemplo, y los procedimientos desglosados en diferentes tópicos que en su conjunto permiten explorar el entorno informático de una organización.

1. FUNDAMENTOS TEÓRICOS

1.1 CONCEPTOS DE AUDITORIA

1.1.1 Auditoría informática

Es la evaluación y verificación de las políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección), a fin de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Según José A. Echenique, la auditoría en informática:

> Es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.
>
> La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización especifica que hará posible el uso de los equipos de cómputo[1].

[1] ECHENIQUE, José Antonio. Auditoría en informática. México, McGraw Hill, 2001 p. 16.

Según Mario Piattini Velthuis, la auditoría informática es "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos"[2].

Con base en los conceptos anteriores, se puede afirmar que realizar una auditoría informática y de sistemas es la evaluación que un profesional de auditoría realiza a las normas, controles, sistemas de información, funciones, procedimientos, software, hardware y talento humano desde el punto de vista administrativo, técnico y de seguridad, buscando siempre que las empresas apliquen controles que los lleve a proporcionar: confiabilidad, oportunidad de mejoramiento, seguridad, confidencialidad y eficiencia que faciliten a la parte administrativa la toma de decisiones.

1.1.2 Auditoría de Sistemas

Desde el punto de vista administrativo, cuando se habla de auditoría de sistemas se refiere a los sistemas de información utilizados en las empresas públicas o privadas, mas no al computador como tal, que en sí es una herramienta utilizada para el manejo de la información. Se debe tener presente que la administración es un sistema abierto y por tanto cambiante en sus conceptos, técnicas y que está influenciada por lo que acontece en su alrededor.

> La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los no automáticos relacionados con ellos y las interfaces correspondientes; también se puede decir que es el examen y evaluación de los procesos del área de Procesamiento Electrónico de Datos (PED) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia,

[2] PIATTINI, Mario. Auditoria de tecnologías y sistemas de información. Cali Grupo Editorial Alfaomega, 2008. p. 7.

efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas[3].

Según lo anterior la auditoria de sistemas puede aplicarse a cualquiera de los sistemas de información que se usen funcionalmente en la organización y cualquier sistema de información en desarrollo dentro de la organización. También se entiende que la auditoria de sistemas incluye implícitamente a los recursos informáticos que soportan el sistema.

1.2 OBJETIVOS GENERALES DE LA AUDITORÍA INFORMÁTICA Y DE SISTEMAS

Los objetivos generales de la auditoria Informática y de sistemas son los siguientes:

- Analizar los mecanismos adoptados para proporcionar la protección de los activos y la integridad de los datos.
- Asesorar a la gerencia y a los altos directivos de la empresa en lo relacionado con los sistemas de información, de tal forma que el proceso de toma de decisiones se efectúe lo más acertadamente posible.
- Analizar la concepción, implementación y funcionalidad de la seguridad aplicada a los sistemas de información.
- Evaluar las políticas generales adoptadas para garantizar la seguridad física, lógica y planes de contingencia que garanticen la continuidad del negocio.

1.3 OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA INFORMÁTICA Y DE SISTEMAS

Los objetivos específicos de la auditoria Informática y de sistemas son los siguientes:

[3] RESTREPO A. Jorge A. GUÍA PARA LA CLASE DE AUDITORIA DE SISTEMAS (en línea). En. El blog de la Comunidad de Coomeva, Abril, 2010. (Consultada el 10 de Agosto del 2011) disponible en la dirección electrónica: http://jorgearestrepog.comunidadcoomeva.com/blog/index.php

- Evaluar los procedimientos para captura, verificación, almacenamiento de los datos y para asignación de claves de acceso, modificaciones y cancelaciones.
- Analizar las políticas para la adquisición y/o desarrollo de software.
- Examinar la documentación existente con respecto a los manuales de sistemas, usuarios, operación, funciones y procedimientos para determinar actualizaciones y efectividad.
- Revisar los procedimientos existentes sobre seguridad física con respectos a instalaciones, personal y equipos.
- Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de los funcionarios de una institución así como evaluar las actividades que se desarrollan en sus áreas y unidades administrativas.
- Comprobar si los planes de seguridad son evaluados periódicamente.
- Evaluar si existe una adecuada segregación de funciones y su cabal aplicación.

1.4 CONTROL INTERNO INFORMÁTICO

1.4.1 Control

"Es el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales" [4]

La ley 87 de 1993 en su artículo 1, define el Control Interno como: "el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales, legales y vigentes dentro

[4] TAMYO ALZATE, Alonzo. Auditoría de Sistemas: Una visión práctica. Manizales; Centro de publicaciones Universidad Nacional de Manizales, 2002. p. 14.

de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos"[5].

El control debe ser ejecutado frecuentemente para que permita identificar las oportunidades de mejoramiento a tiempo y poder tomar las decisiones a tiempo; los beneficios que arroje deben ser superiores a los costos de implantación y mantenimiento del mismo. El proceso de control debe corresponder a una planeación que permita conocer la magnitud de la acción correctiva necesaria, el control deber ser en la medida de lo posible sencillo, comprensible y adaptativo, donde su aplicación no entorpezca el desarrollo normal de la empresa.

1.4.1.1 *Control interno*

El control interno es un proceso llevado a cabo por las personas de una organización, diseñado con el fin de proporcionar un grado de seguridad razonable para la consecución de sus objetivos. Este proceso debe ser impulsado al interior de las organizaciones por las directivas y administradores quienes designan una persona o grupo que posee la suficiente ética, moral y formación académica que le amerita credibilidad para que ejerza esta función.

1.4.1.2 *Control externo*

El control externo como su nombre lo indica, es ejercido por personal externo a la empresa y su propósito es evaluar en qué proporción las metas y objetivos trazados en las políticas, planes, programas por la administración de la misma se están cumpliendo.

Los principales objetivos del control interno son los siguientes:

- Controlar que todas las actividades se realicen cumpliendo con los procedimientos y normas fijados
- Evaluar la bondad de cada uno de los controles
- Asegurar el cumplimiento de normas legales
- Asesorar sobre el conocimiento de las normas

[5] CONGRESO DE COLOMBIA. LEY 87 DEL 29 DE NVIEMBRE DE 1993. (en línea). UNIVERSIDAD DEL VALLE. Noviembre, 1993. Consultada el 17 de Agosto del 2011. Disponible en la dirección electrónica: http://controlinterno.univalle.edu.co/doc/ley_87_1993.pdf.

- Colaborar y apoyar el trabajo de la auditoría
- Colaborar en las auditorias externa
- Definir, implantar y ejecutar mecanismos de control interno
- Comprobar el logro adecuado de prestación de los servicios
- Implantación de mecanismos de medida y responsabilidad del logro de niveles de servicio adecuados

1.4.2 Control Interno Informático

El control interno informático controla diariamente que todas las actividades de sistemas de información se realicen cumpliendo con los procedimientos, estándares y normas fijados por la dirección de la organización y/o dirección informática para el cumplimiento de los requerimientos legales. Generalmente la función de control interno informático suele ser un órgano "staff" de la dirección de departamento de informática o sistemas.

El establecimiento de controles internos en el área informática y los sistemas de información es muy importante, ayuda a la evaluación de la eficiencia y eficacia de la gestión administrativa, dependiendo de los objetivos que se pretenda con los controles. Además, el control interno es indispensable en la protección de los bienes y el buen desarrollo de las actividades y operación de los sistemas.

A través del control interno se pretende la aplicación de los siguientes objetivos específicos:

- Establecer como prioridad la seguridad y protección de los bienes informáticos, la información y los sistemas de información.
- Promover la confiabilidad, oportunidad y veracidad de la captura de datos, su procesamiento y la emisión de reportes en la empresa.
- Implementar los métodos, técnicas y procedimientos necesarios para contribuir al desarrollo eficiente de las funciones, actividades, y tareas de los servicios que presta el área informática para satisfacer las necesidades de la empresa.
- Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
- Establecer acciones necesarias para el buen desarrollo del software, a fin de que presten un buen servicio en la empresa.

El control en los sistemas de información pretende verificar que los datos sean reales, exactos, oportunos, suficientes y sobre todo que no se vean afectados por pérdida, omisión o redundancia, que proporcionen la información requerida.

Los controles en los Sistemas de Información se pueden clasificar en: Controles generales, operativos y técnicos.

Generales: Son aquellos ejercidos sobre las actividades y recursos comprendidos en el desarrollo de los sistemas.

Operativos: Son aquellos diseñados, desarrollados e implementados para sistemas específicos, buscando garantizar con ellos que todas las operaciones sean autorizadas, registradas y procesadas de una manera completa exacta y oportuna.

Técnicos: Tienen que ver con la tecnología de la información y son aplicables al hardware, software, sistemas de mantenimiento y planes de contingencia.

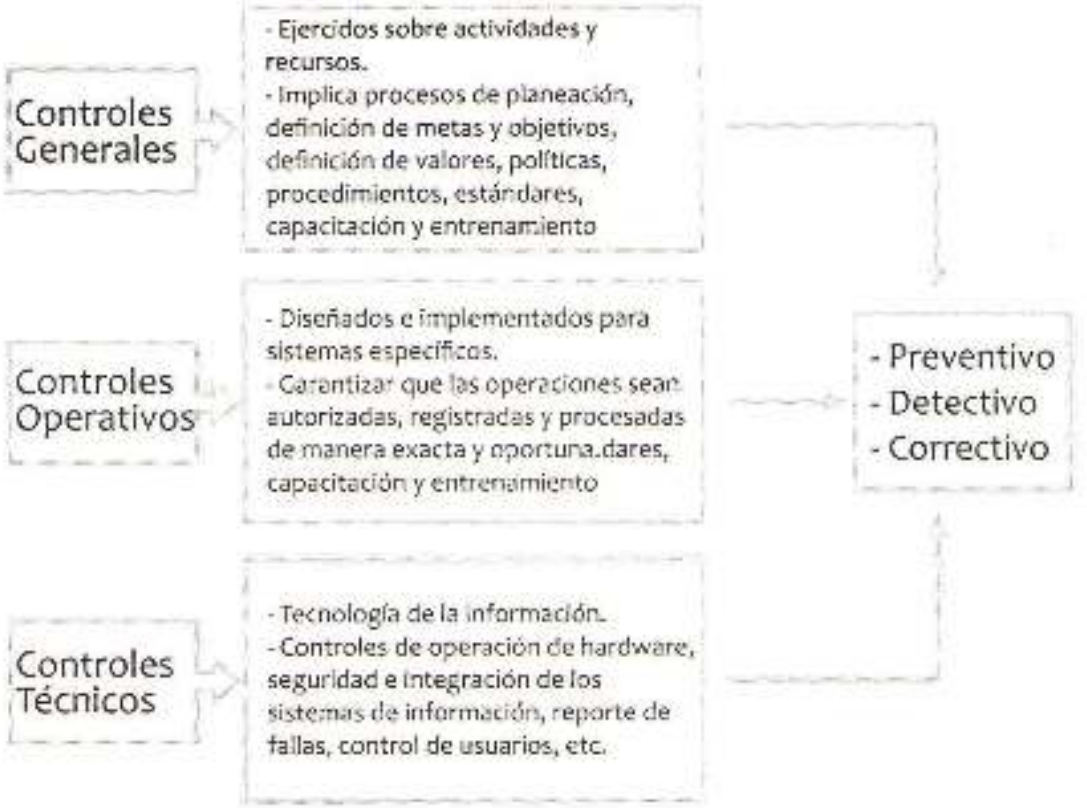
Otra de las taxonomías de controles los clasifican teniendo en cuenta si las acciones se llevan a cabo antes, durante o después del evento, de acuerdo a esta clasificación los controles pueden ser:

Preventivos: Cuando están involucrados dentro de los procesos y tienen como propósito evitar la ocurrencia y frecuencia de incidencias

Detectivos: Que se activan una vez se registra la ocurrencia de la incidencia y tienen como propósito alertar a las personas involucradas en el proceso.

Correctivos: Que se ejecutan para tomar acciones correctivas, cuando ha ocurrido la incidencia.

Figura 1: Clasificación de Controles



Fuente: Esta Investigación

1.5 PAPELES DE TRABAJO

Son la herramienta y soporte en la planeación, organización y coordinación del examen de auditoría, y a su vez brindan respaldo a la opinión del auditor. Estos se preparan de acuerdo al criterio, experiencia y preferencia del auditor, se organizan teniendo en cuenta su uso y contenido.

Según José Dagoberto Pinilla define los papeles de trabajo así: "comprende el conjunto de cedulas preparadas por el auditor y/o personal colaborador, con motivo del desarrollo del programa de auditoría para obtener evidencia comprobatoria suficiente y competente, que sirva como base objetiva para emitir una opinión independiente sobre el objeto auditado"[6].

[6] PINILLA FORERO, José Dagoberto. Auditoría Informática: Un Enfoque Operacional. Ed Eco Ediciones, Colombia. 1992. p. 50.

Los papeles de trabajo son registros que mantiene el auditor de los procedimientos aplicados, pruebas desarrolladas, información obtenida y conclusiones pertinentes a que se llegó en el trabajo. Algunos ejemplos de papeles de trabajo son los programas de auditoría, los análisis, los memorandos, las cartas de confirmación y declaración, resúmenes de documentos de la compañía y cédulas o comentarios preparados u obtenidos por el auditor, los papeles de trabajo también pueden obtener la forma de información almacenada en cintas, películas u otros medios.

1.5.1 Objetivos de los Papeles de Trabajo

En las normas técnicas de auditoría se establece que los principales objetivos de los papeles de tabajo son los siguientes:

- Proporcionar la información básica y fundamental necesaria para facilitar la planeación, organización y desarrollo de todas las etapas del proceso de auditoría.
- Respaldar la opinión del auditor permitiendo realizar un examen de supervisión y proporcionando los informes suficientes y necesarios que serán incluidos en el informe de auditoría, además, sirve como evidencia en caso de presentarse alguna demanda.
- Permiten demostrar si el trabajo del auditor fue debidamente planeado, determinando su eficiencia y eficacia.
- Permiten establecer un registro histórico disponible permanentemente en caso que se presente algún requerimiento.
- Servir como punto de referencia para posteriores auditorías.
- Servir de puente entre el informe de auditoría y las áreas auditadas.

1.5.2 Propiedades de los Papeles de Trabajo

La guía internacional de auditoría No.9 documentación. Señala en los párrafos 12 y 13 lo siguiente:

Párrafo 12 "los papeles de trabajo son de propiedad del auditor. Este puede, a su criterio, poner a disposición de su cliente parte