GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO

MARIO OROZCO BOHÓRQUEZ
UBALDO MARTINEZ PALACIO
WILLIAM TORRES ROYERO

CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC
ESPECIALIZACIÓN DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA
2010

GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO.

MARIO OROZCO BOHÓRQUEZ
UBALDO MARTINEZ PALACIO
WILLIAM TORRES ROYERO

Trabajo de grado presentado como requisito para optar al título de Especialista en Auditoría de Sistemas de Información

Director:
Ing. VICTOR MANUEL MONTAÑO ARDILA

CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC
ESPECIALIZACIÓN DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA
2010

PAGINA DE ACEPTACION

Nota de aceptación

_____
_____
_____
_____

_____

Jurado

_____

Jurado

Barranquilla, Octubre de 2010

RESUMEN

La adquisición de software hoy en día es una de las principales estrategias que adoptan las organizaciones. En lo relacionado a las tecnologías de Información (TI) el índice de fracaso en cuanto a proyectos de software, sobrepasa el 50%.

Este fracaso esta relacionado con dos causas principales:

1. Fallas en la Gestión de proyectos de adquisición de software o carencia del mismo. El proceso de Gestión de Riesgos en una organización es un punto clave para atacar de raíz la causa de fracaso mencionada con anterioridad.

2. La complejidad de los Estándares y Modelos de Gestión de Proyectos que dificulta su implementación.

La presente tesis tiene como finalidad diseñar una Guía Metodológica para Pequeñas y Medianas Empresas del Sector Privado que deseen ejecutar o mejorar el proceso de adquisición de software, permitiendo así la reducción de los problemas que de alguna u otra manera afecten el éxito la ejecución de dicho proceso.

El trabajo se realizo en base a tres estándares de buenas practicas como son: ISO 9000, CobiT 4.1 y el documento Information Technology: An Audit Guide for Assessing Acquisition Risks (Tecnología de la Información: Una guía de auditoría para la evaluación de los riesgos de Adquisición).

El trabajo se desarrollo en tres etapas: en la primera se enmarco la investigación en las disciplinas que de alguna u otra forma apuntaran al proceso de adquisición de software, y por medio de estas se define el contexto del problema, el estado del

arte y la realización de una revisión sistémica que justifica y apoya el estado del arte antes mencionado. En la segunda etapa se recogen los datos mediante encuestas para soportar la investigación, haciendo referencia a ciertos ítems a tener en cuenta, obtenidos de los estándares anteriormente mencionados. Y en la etapa final se realizo un capitulaje especial llamado guía metodología en la que se obtuvo la guía en mención en el proyecto.

ABSTRACT

The acquisition of software today is one of the main strategies adopted by organizations. In regard to information technology (IT) the rate of failure in software projects, is over 50%.

This failure is related to two main causes:

1. Failures in project management software acquisition or lack thereof. The Risk Management process in an organization is key to tackling the root causes of failure mentioned above.
2. The complexity of the standards and management models that hampers their implementation projects.

This thesis aims to design a Methodological Guide for Small and Medium Private Sector Companies wishing to implement or improve the software acquisition process, thereby reducing the problems that one way or another affect the successful implementation of the process.

The study was conducted on three standards of good practice such as ISO 9000, COBIT 4.1 and document Information Technology: An Audit Guide for Assessing Acquisition Risks (Information Technology: A guide for assessing audit risk acquisition).

The work took place in three stages: the first was framed research in disciplines that one way or another will point to the software acquisition process, and through these we define the context of the problem, the state of the art and conducting a systematic review that justifies and supports the state of the art above. In the second stage data is collected through surveys to support the investigation, with

reference to certain items to be taken into account, obtained from the above standards. And in the final stage was made a special chapter call methodology guide in order to obtain the guide mentioned in the project.

AGRADECIMIENTOS

A Dios creador del universo y columna vertebral de todas las metas y objetivos propuestos en mi vida.

A mi Esposa Dra. Silvana Beatriz Ramírez mejía por creer en mí y estar siempre a mi lado apoyándome y dándome aliento en los momentos difíciles de mi vida.

A mis Hijos Mario Edgardo Orozco Ramírez y Alberto Mario Orozco Ramírez porque son la luz de mi vida y la principal fuente de energía para seguir adelante sin desfallecer en ningún momento.

A mi madre, Marlene María Bohórquez Jiménez por su apoyo a lo largo de toda mi vida personal y profesional.

A mis suegros, Dr. Edgardo Allan Ramírez Acosta y la Dra. Magaly del Carmen Mejía Miranda por su contante apoyo en todas y cada una de las etapas de mi vida.

A la Corporación Universitaria de la Costa CUC por su apoyo y por hacer posible la realización de esta investigación.

A los docentes de cada uno de los módulos de la Especialización de Auditoría de Sistemas de Información, que de una u otra forma sembraron su granito de arena para brindar conocimiento Y a todas aquellas personas que colaboraron o participaron en la realización de esta investigación, hago extensivo mi más sincero agradecimiento.

(Ing. Mario Orozco Bohórquez)

AGRADECIMIENTOS

Le agradezco infinitamente a **Dios**, creador de la vida, quien es en quien confío para alcanzar todas mis metas y a quien nombro de manera prioritaria por la importancia en mi vida y porque me encomiendo mucho a él en todas mis metas, como efecto de esto, ya estoy por cumplir uno de mis grandes sueños.

A mis padres, William Torres Torres y Neifa Royero Gómez, que en realidad aquí en la terrenalmente son quienes fueron quienes me apoyaron tanto emocional y monetariamente, su apoyo incondicional y con el ánimo de sacar a su hijo adelante, me da el gusto de agradecerles por el resto de la vida por dejarme ser lo que soy sin ninguna restricción.

A mi hermana Sandra Johana Torres Royero por ser tan linda conmigo y estar a pesar de todo en las buenas y las malas.

A mis amigos: Gina Paola Herrera Rodríguez, Claudia Ramírez T., Néstor Chamorro Esparragoza, Jeimi D'Andreis Hernández, Laura Vásquez, Claudia Vargas, Justine Torres Rodríguez, Karen Vásquez, María Uran Ruidiaz, Alexis de la Hoz y Ubaldo Gil Colón; quienes estuvieron al tanto de mi proceso de la especialización de Auditoría de Sistemas de Información.

A la excelente calidad de personas y profesionales que nos capacitaron en esta aventura, estoy hablando de los Docentes, que fueron los que nos llenaron de su conocimiento para ser unos Auditores exitosos, que Dios los bendiga donde estén
Y por último a todas las personas que directa e indirectamente pusieron su granito de arena y colaboraron para la consecución de mi post grado.

(Ing. William Manuel Torres Royero)

AGRADECIMIENTOS

A Dios que me ha brindado la posibilidad de superarme y alcanzar mis metas, que me ha bendecido infinitamente y protegido con su preciosísima sangre y en los momentos mas difíciles de mi vida ha estado conmigo y no me ha desamparado.

A mis padres Rosario Palacio y Menelao Martínez quienes se han sacrificado para hacer de mí, un hombre de bien, con muy buenos valores y principios, y me han ayudado a salir adelante con sus consejos y buenas energías.

A todos mis demás familiares, amigos y conocidos que de alguna u otra forma me ayudaron y confiaron en mí.

A cada uno de los profesores de la especialización quienes con su sabiduría y conocimiento infundieron en mí un profundo agrado por la auditoria y las buenas practicas.

A mis demás familiares, amigos y conocidos, porque de alguna u otra forma me colaboraron cuando necesité una mano amiga.

Por todo lo anterior y por mucho mas agradezco infinitamente alcanzar este gran logro.

(Ing. Ubaldo José Martínez Palacio)

GLOSARIO

- ***Actividad**:* Cualquier paso o función que se realiza (mental o física) para alcanzar algún objetivo.

- ***Área clave de proceso:*** Grupo de actividades relacionadas que cuando se llevan a cabo en conjunto alcanzan un conjunto de metas (consideradas importantes para aumentar la capacidad del proceso). KPAs

- ***Capacidad de un proceso:*** Rango de resultados esperados que se pueden obtener tras seguir un proceso.

- ***Caja negra cerrada:*** Solución de Tecnologías de información, donde no se conoce su funcionamiento interno, el código fuente no es entregado y no es posible su intervención por terceros.

- ***Caja negra modificada o parametrizada*****:** Solución de Tecnologías de información, donde no se conoce su funcionamiento interno, el código fuente no es entregado y es posible su intervención por terceros y su parametrización.

- ***CMM:*** Capability Maturity Model. Es una metodología que describe elementos claves de un proceso de software eficaz, describe una ruta de mejoramiento evolutivo para pasar desde un proceso inmaduro a un proceso maduro y disciplinado, basado en conicimiento9s adquiridos de evaluaciones de los procesos de software y extensas retroalimentaciones con el entrono donde interactúa la organización.

- ***COBIT:*** Control Objetive for Information and related Techonogy. Es una entidad que proporciona unos principios para los administradores de proceso que se desarrollan en Tecnologías de información y que deben responder de manera eficiente y efectiva tanto para el negocio de la organización como para su control.

- ***"Firewall"*** == ***Contrafuego****:* Un cortafuegos es una barrera para evitar que el fuego se expanda. Los edificios disponen de cortafuegos, muros de ladrillos que dividen las diferentes secciones del edificio. En un coche, un cortafuego es la plancha de metal que separa al motor del compartimiento de los pasajeros. La misión de los cortafuegos de Internet es garantizar la seguridad de nuestro equipo ante los peligros cibernéticos de la red de área local (LAN) o bien, mantener a los miembros de esa LAN al margen de las malignas intenciones de Internet.1

- ***Institucionalizar:*** Identificar una infraestructura y una cultura que soporte los métodos, las prácticas y los procesos para que estos sean la manera real de hacer negocios.

- ***ISO: International Organization for Standardization. Conjunto de normas y directrices internacionales para la gestión de calidad.***

- ***Lista de chequeo:*** Serie de pasos, secuenciales y relacionados entre sí en ocasiones, los cuales proveen información sobre el correcto funcionamiento de procesos, sistemas y comportamientos.

- ***Madurez de un proceso de software*****:** Punto en el cual un determinado proceso es explícitamente definido, administrado, medido, controlado y efectivo.

---

1 http://ibiblio.org/pub/Linux/docs/HOWTO/translations/es/Cortafuegos-COMO.gz

- ***Nivel de Madurez*:** Plataforma bien definida desde la cual se obtiene un proceso maduro de software. Grado de institucionalización y pertenencia que puede llegar a tener un proceso o proyecto en el diario vivir de la organización.

- ***Outsorcing*:** Mecanismo de provisión de servicios.

- ***Proceso de Software*:** Conjunto de actividades, métodos, prácticas y transformaciones para desarrollar, y mantener software y productos asociados.

- ***Propiedad emergente:*** Características que surgen y se desarrollan a medida que un sistema es coherente, autorregulado y autónomo; dichas características no son tangibles.

- ***Rendimiento del los procesos de software*:** Resultados actuales logrados siguiendo los procesos de software.

- ***Recursos IT:*** Datos, sistemas aplicativos, tecnología, facilitadores y personal.

- **RFP:** Un **RFP** (**Request for proposal, o solicitud de propuesta**) es un documento que una empresa emite para solicitar propuestas de posibles proveedores de productos o servicios. Por ejemplo, una empresa que desee digitalizar su información, podría solicitar propuestas que incluyan equipos, programas, y el entrenamiento de los usuarios requeridos para operar el sistema e incorporarlo en la organización. Otra empresa podría requerir una propuesta para el desarrollo de una aplicación en particular.

  Las **RFP** son un componente vital en la administración de proyectos exitosos ya que definen claramente los entregables asociados con el proyecto y define un marco de acción para la ejecución del mismo. Idealmente los RFP estipulan

los requisitos de la empresa que está comprando y las condiciones bajo las cuales contrataría, por lo que un RFP debe contener:

1. Especificación del producto o servicio requerido, con el mayor detalle posible
2. Información que se requiere del oferente, como el valor, las personas que liderarán el proyecto, responsabilidades que asumirá, un cronograma, y la experiencia de la empresa en el área, por ejemplo
3. Criterios para selección o descalificación de proponentes
4. Fechas relevantes, incluyendo las de apertura y cierre del proceso. Fechas para entrevistas y visitas si las hay.
5. Cualquier requerimiento de confidencialidad.
6. Elementos legales de la posible contratación.

Un RFP se convierte en parte del proceso de compras de una organización, el cual inicia con la evaluación de las necesidades y termina con la entrega del producto o servicio.

- ***Stakeholders*:** Grupos de interés participantes de forma indirecta o directa en el desarrollo de un proceso. Definir de manera correcta estos grupos influye en el éxito y fortalezas del proceso o proyecto.

TABLA DE CONTENIDO

Pág.

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

INTRODUCCION

En la actualidad gran parte del valor agregado de una organización se ve reflejado en el personal que labora, herramientas tecnológicas y sus sistemas de información.

En la actualidad las empresas se han esmerado por mantener sus productos o servicios en el mercado y de esa manera poder subsistir. Con la llegada de la tecnología las empresas han sentido un apoyo en sus negocios y les ha permitido incursionar en mercados antes imposibles de acceder.

El impacto en el día a día de la tecnología a través del proceso de adquisición de software ha sido de gran alcance, debido a que esto les ha permitido cumplir con sus metas organizacionales.

El hablar de software implica ciertas actividades como son: requerimientos, búsqueda de diversas alternativas en el mercado, evaluar propuestas de proveedores, capacitación de personal, instalación e implementación, costos, mantenimientos, etc.

El problema de la adquisición de software hace referencia a la adecuada escogencia de éste, a la adecuada inversión de un software a medida para la organización y que permita la integración de los diversos procesos manejados en la empresa y que sea adaptable a los cambios en ésta.

Existen entidades internacionales reconocidas que han diseñados estándares, metodologías, normas, modelos y/o directrices, enfocados en seguridad, desarrollo, adquisición etc. Entre las principales se puede mencionar: SEI (Software Engineering Institute - Instituto de Ingeniería de Software), IEEE

(Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos), ISO (International Organization for Standarization - Organización Internacional de Estandarización) y también SPICE (Software Process Improvement and Capability Determination – Mejoramiento de procesos de Software y determinación de capacidad).

La ISO presenta una colección de estándares enfocados a la calidad, siendo la ISO 9001 la que esta orientada al software en lo que se refiere al desarrollo y manutención, y adicionalmente forma parte de la serie ISO 9000. La ISO 9000-3 (IBNORCA 1998) del año 1997 es una guía al aplicar ISO 9001 del año 1994 para el desarrollo, provisión y mantenimiento de software. Esta experimento nuevas versiones como es el caso de ISO 9003 del año 2004 (ISO/IEC 2004) que es la guía de aplicación de la ISO 9001 del año 2000 para software de computadora. Otro estándar relacionado al software es la ISO/IEC 12207:1995 (ISO/IEC 1995) que establece un marco de referencia común para los procesos del ciclo de vida del software.

Dentro de los desarrollos del SEI podemos describir a SW-CMM (SEI 1993) (Software Capability Maturity Model - Modelo de Madurez de Capacidad de Software), SA-CMM (SEI 2002a)(Software Acquisition Capability Maturity Model - Modelo de Madurez de Capacidad para la Adquisición de Software), CMMI (SEI 2002b, SEI 2002c) (Capability Maturity Model Integrated - Modelo de Capacidad de Madurez Integrado) y CMMI – AM (SEI 2005) (CMMI Adquisition Module -l Modulo de Adquisición para CMMI).

La IEEE presenta muchos estándares relacionados o involucrados con la calidad de software como son: 610.12-1990 que es el glosario estándar de terminología de ingeniería de software, 730-1998 que es el estándar para planes de seguridad de calidad de software, 829-1998 estándares para documentar la evaluación de software, 830-1998 practicas recomendadas para especificación de

requerimientos de software, 1012-1998 estándar para la verificación y validación de software 1016-1998 practicas recomendadas para la descripción de diseño de software, 1062a-1998 practicas recomendadas para la adquisición de software y muchas otras más.

1. PLANTEAMIENTO DEL PROBLEMA

El proceso de adquisición de software representa hoy día una de las principales estrategias que adoptan las organizaciones para optimizar o automatizar todos y cada uno de los procesos existentes dentro de ella.

En este proceso intervienen diversos factores, pero uno de los más importantes se refiere a la parte económica y a como identificar si en realidad estoy adquiriendo un producto que va a traer beneficios de una u otra forma a la organización.

Se ha determinado según estudios que aproximadamente el 50% de la adquisición de software en las organizaciones fracasa y este fracaso está estrechamente relacionado a:

1. Fallas en la Gestión de proyectos de adquisición de software o carencia del mismo. El proceso de Gestión de Riesgos en una organización es un punto clave para atacar de raíz la causa de fracaso mencionada con anterioridad.

2. La complejidad de los Estándares y Modelos de Gestión de Proyectos que dificulta su implementación.

La intención de adquirir un software radica en que éste automatice muchos procesos que se manejan en la organización con el fin de incrementar la eficiencia y efectividad en estos y así obtener mayores beneficios a la misma.

Los problemas que normalmente se presentan a la hora de someter a la organización a un proceso de adquisición de software son los siguientes:

- Altos costos
- Incumplimiento de cronograma
- Relación pobre entre cliente y proveedor
- Productos inexequibles
- No atendimiento de las necesidades y expectativas del usuario
- No cumplimiento de los requisitos especificados
- Dificultades de personalización del software
- Pérdida de control del proyecto
- Falta de acompañamiento del proyecto
- Falta de visibilidad de los procesos subcontratados
- Ciclo desarrollo muy largo
- Falta de habilidad de previsión problemas
- Dificultad en la prevención de defectos
- Baja disponibilidad de recursos humanos
- Alta rotación del personal

2. JUSTIFICACIÓN E IMPORTANCIA DEL ESTUDIO

2.1 BENEFICIO ORGANIZACIONAL

Se dice que el futuro de una organización está estrechamente relacionado con que estas requieran calidad en sus servicios y la tecnología de información, mas que todo el software lo que busca en maximizar la flexibilidad y el control sobre los procesos. Por ende el éxito o fracaso de un proyecto de adquisición depende estrictamente de la gestión que se lleve a cabo en dicho proyecto.

Los procesos de adquisición de software son cada vez más usuales porque es un recurso vital para todo tipo de organizaciones. Existen diferentes formas de obtener o adquirir software como son: Por desarrollo interno, desarrollo por contrato (tercerizado) o mediante la compra de un producto ya elaborado. En el proceso de adquisición de software se pueden observar dos roles principales, el rol del adquiridor o comprador y el rol del proveedor o desarrollador.

En el instante que una organización implemente un proceso de adquisición de software tendrá la oportunidad de evaluar todos y cada uno de los ítems relacionados a este proceso y podrá tomar decisiones basado en una evaluación más concreta y certera para minimizar al máximo la posibilidad de perder dinero y tiempo a la hora de seleccionar el producto deseado.

2.2 BENEFICIO ECONÓMICO

Muchas veces la organizaciones hacen inversiones prácticamente a ciegas. Efectúan compras de productos de software de manera esporádica e intuitiva, más que siguiendo un plan específico que refuerce su flanco tecnológico.

Posteriormente se ven forzados a seguir invirtiendo para actualizar sus equipos o simplemente identifican que el aplicativo no satisface todos los requerimientos de información y/o comunicaciones para que todo funcione como lo esperaban y necesitaban.

De acuerdo al crecimiento que ha tenido y la actual tendencia a implementar procesos de adquisición de software en las organizaciones se ha determinado que el ahorro o el beneficio económico a la hora de dicha implementación es bastante significativo, ya que mediante este proceso podremos determinar si realmente el producto cumple con los requerimientos del negocio, ayuda al cumplimiento de las metas y objetivos de la organización y reduce el problema que afecta el éxito de un proceso de adquisición de software en la actualidad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Aplicar los conocimientos adquiridos en la especialización de auditoría de sistemas de información, para diseñar una Guía Metodológica que permita solucionar la problemática del proceso de adquisición de software para pequeñas y medianas empresas del sector privado.

3.2 OBJETIVOS ESPECÍFICOS

- Determinar la importancia de la implementación de una guía metodológica para el proceso de adquisición de software en las organizaciones.
- Identificar el personal involucrado en dicho proceso y que rol debe cumplir cada uno de ellos**.**
- Identificar necesidades, requerimientos y especificaciones.
- Determinar cual es la alternativa o proveedor más óptimo para la organización.
- Identificar lo que hay que tener en cuenta para construir un plan de adquisición que me permita proyectar el éxito en la organización.
- Identificar toda la documentación a tener en cuenta en un proceso de adquisición de software antes de la selección. (Propuesta, Cotización, licitación, etc.).
- Identificar los puntos claves a tener en cuenta para la administración de dichos contratos.
- Identificar los requisitos a tener en cuenta para la aceptación y aprobación de la propuesta.
- Identificar requerimientos a tener en cuenta a la hora de instalar el software.

4. ALCANCE

Utilizando metodologías ya existentes en el mercado para el proceso de adquisición de software en las organizaciones, la revisión y evaluación del estado actual del proceso antes mencionado, se generará una Guía Metodológica propia y específica para la adquisición de software para las organizaciones medianas y pequeñas, con base en el documento **Information Technology: An Audit Guide for Assessing Acquisition Risks** (Tecnología de la Información: Una guía de auditoría para la evaluación de los riesgos de Adquisición), con el apoyo de **CobiT 4.1**, e **ISO 9000:2008.**

Lo importante es que basado en la metodología, las organizaciones sean capaces de identificar si en realidad el producto que se va a adquirir es capaz de entregar soluciones óptimas y adecuadas al negocio, si se va a implementar la solución en el tiempo estipulado para hacerlo, si los sistemas trabajarán de manera óptima cuando se implemente la nueva solución y si los cambios que se realicen sobre la parte tecnológica afectarán de alguna manera las operaciones del negocio.

5. MARCO DE REFERENCIA

5.1 MARCO TEÓRICO Y ESTADO DEL ARTE

A la hora de realizar una inversión de software, la base de una buena decisión no debe hacerse en base de exclusiones a priori de las tecnologías que actualmente se encuentren disponibles, que puedan satisfacer las necesidades de la organización.

La organización de tener la seguridad de adquirir una solución de software con el valor máximo por la suma de dinero que se ha invertido, en contraposición a la necesidad de la organización sin importar que esto implique utilizar soluciones de software cuya propiedad sea exclusiva o cuyas fuentes sean abiertas.

Para tomar una decisión realmente fundamentada, es de vital importancia la realización de un análisis Costo-Beneficio bien diseñado que incluya un modelo de costo total de una propiedad.

Generalmente, las decisiones sobre adquisiciones de software son decisiones de inversión, que si se mantienen debidamente, puede generar durante muchos años grandes beneficios. Por lo tanto estas decisiones deben tomarse en base a los beneficios y costos que se acumulan a lo largo del ciclo de vida de la adquisición.

Los datos arrojados por los diferentes sistemas de información sirven de apoyo en las estrategias que conllevan al óptimo cumplimiento de las metas y objetivos organizacionales. Los sistemas de información pueden alimentarse de datos (fechas, cifras, texto) que de alguna u otra manera son datos simples que pueden o no tener relación entre sí, pero estos también se pueden alimentar y formar parte de un sistema de gestión.

La estrategia principal de una organización es ajustarse simultáneamente a las expectativas de los Stakeholders1 y los recursos en capacidad de respuesta a los cambios que el entorno produce, siendo planteada de una forma ágil y practica siempre y cuando se conozcan en la organización desde la perspectiva interna y externa. El cambio de la estrategia debe ser un proceso continuo de ajustes pequeños de dicha estrategia o de los controles que existen actualmente en la organización, en los subsistemas que necesiten los cambios.

5.1.1. Cadena de Valor en una organización

La capacidad estratégica de una organización es posible valorarla, gracias a herramientas como análisis de recursos. Esta herramienta se ve reflejada en la utilización de la “Cadena de Valor” cuyas características son:

- Existe una relación entre la capacidad y la forma en que se utilizan y controlan los recursos.
- Está orientada a satisfacer demandas del mercado, a crear productos diferenciados de mayor valor y un compromiso compartido para cumplir con los requisitos del mercado en cuanto a: calidad, trazabilidad, volúmenes, frecuencia.
- Ayuda a comprender la capacidad estratégica de la organización.
- Posee un flujo de información y conocimiento extensivo; relaciones de coordinación, roles y reglas de juego claramente definidas.
- Se concentra en actividades de valor y los vínculos entre estas actividades.
- El reconocimiento de la interdependencia entre actores y colaboración estratégica en búsqueda de la competitividad sistémica. Confianza entre los actores de la cadena, disposición a compartir riesgos y beneficios, y una visión de largo plazo.

La cadena de valor puede tener variantes en el área tecnológica dependiendo el negocio de la organización que se analice, todo esto se debe a que las actividades primaria de la organización pueden estar enfocadas en la atención al cliente o al soporte de equipos o a los dos.

Las actividades primarias que conforman la creación física del producto, las actividades relacionadas con su venta y la asistencia post-venta. Se dividen en:

- Logística interna: recepción, almacenamiento y distribución de las materias primas.
- Operaciones (producción): recepción de las materias primas para transformarlas en el producto final.
- Logística externa: almacenamiento de los productos terminados y distribución del producto al consumidor.
- Ventas y Marketing: actividades con las cuales se da a conocer el producto.
- Servicios post-venta (mantenimiento): actividades destinadas a mantener o realizar el valor del producto. Ej.: garantías

Estas actividades son apoyadas por las también denominadas actividades secundarias:

- Infraestructura de la organización: actividades que prestan apoyo a toda la empresa, como la planificación, contabilidad, finanzas...
- Dirección de recursos humanos: búsqueda, contratación y motivación del personal.
- Desarrollo de tecnología (investigación y desarrollo): obtención, mejora y gestión de la tecnología.
- Abastecimiento (compras): proceso de compra de los materiales.

Existe una relación estrecha entre las necesidades o logística de entrada y el desarrollo, de la comunicación de las anteriores depende el éxito de las estrategias estipuladas o implementadas en la organización para alcanzar las metas.

Un elemento de las relaciones es el proceso de adquisición de software el cual debe responder las expectativas de los Stakeholders.

El proceso de adquisición de software se comporta de la misma manera que un sistema en el que “el todo es mayor que la suma de sus partes” y cuyas partes se interrelacionan entre si.

Al ver el proceso como un sistema es posible observar que este es similar al ciclo de vida de un producto, en la que en cada etapa se requiere de un resultado que es prerrequisito de la siguiente etapa, de esa manera los pasos están relacionados formando una cadena.

De esta manera surgen los factores críticos del proceso, tanto para las actividades primarias como para las de apoyo.

5.1.2. Proceso De Adquisición De Software

El proceso de adquisición de software implica una serie de etapas, que están relacionadas entre si como lo muestra la figura de adquisición de software y estas deben reflejar las necesidades de la organización. De la misma forma estas soluciones se basan tanto en recursos de personal como técnicos.

La importancia del proceso de adquisición de software es mejorar la calidad de los productos o servicios que ofrece la organización y reducir los costos.

Cada organización que tenga pensado implementar este proceso debe cuestionarse acerca de: ¿que software necesitamos?, ya que la respuesta a este interrogante permite asegurar que la compra y utilización de este sea eficiente y efectiva.

Para ayudar a responder esta inquietud, se podría complementar con los siguientes interrogantes:

a. ¿La empresa esta utilizando el software mas adecuado para satisfacer sus necesidades?

b. ¿El personal esta satisfecho con los programas actualmente utilizados en la organización?

c. ¿Existen otros programas que de alguna u otra manera permitirían a la empresa operar eficientemente?

d. ¿Tiene instalado en sus equipos programas que ya no utiliza?
En el proceso de adquisición de software debe integrar los siguientes aspectos:

- Identificar las necesidades de los usuarios, tanto funcionales como no funcionales

- Desarrollar términos de referencia. ¿Qué y como es lo que se necesita?

- Construir un plan de adquisición/subcontratación/desarrollo de software.

- Una lista de cheque útil para determinar la estrategia de adquisición.

- Seleccionar proveedor

- Realizar el seguimiento de un proveedor

- Evaluar la eficiencia de un proveedor

- Aceptar los productos entregados por el proveedor de acuerdo con los requerimientos especificados previamente en los Términos de Referencia

- Realizar la transición al uso de los productos.

- Pruebas.

- Mantenimiento correctivo, preventivo y adaptativo.

- Soporte a usuarios.

- Capacitación a administradores y usuarios del producto

- Documentar todos los procesos y actividades para conducir una sesión de lecciones aprendidas para un proyecto que involucra la adquisición de software a terceros.

5.1.3 Como Adquirir Software

En un proceso de software, la calidad y capacidad de este de alguna u otra forma afecta:

- El rango de resultados esperados que pueden ser alcanzados por una organización si hace su propio software.

- Habilidad de una organización para desarrollar y mantener software de alta calidad, entregada a tiempo y dentro de los costos estimados.

La calidad de software es un factor que se puede mejorar si considerablemente se mejora el proceso de adquisición. Las características que debe cumplir cualquier proceso de adquisición son:

- Satisfacer las necesidades de los usuarios.
- Contar con la robustez requerida para su confiabilidad.
- Ser entregado a tiempo y dentro de lo presupuestado.

La organización puede examinar la posibilidad de permitir dejar en manos de terceros procesos automatizados los cuales no hacen parte del núcleo del negocio, es decir, de aquellos procesos que son estándares y se cumplen en todas las empresas de tal manera que mediante "outsourcing"3 o acompañamientos se puedan realizar estas labores.

5.1.4. Modelos Y Estándares Relacionados A La Adquisición De Software

Basándonos en los conocimientos adquiridos a lo largo de la especialización y mediante una investigación acerca del tema del Proceso de Adquisición de Software, fueron seleccionados los siguientes estándares:

- Estándar ISO/IEC 12207
- Estándar IEEE 1062
- Modelo CMMI-ACQ
- Modelo eSCM-CL
- CobiT (dominio Adquirir e Implementar)
- ISO 9000

- ISO 27001
- GAO

Cuyo estudio se realizo de acuerdo al siguiente enfoque:

- Alcance o enfoque del estándar
- Principios básicos
- Fases que componen el modelo

A través de los estándares antes mencionados se determinaran aspectos de la adquisición de software que estos contemplan.

5.1.5. Estándar ISO/IEC 12207[9]

En Junio de 1989 se dio el inició el desarrollo de un estándar internacional ISO/IEC 12207 relacionado con la definición de los procesos del ciclo de vida de software, su interfaz con otros procesos y las relaciones a alto nivel que gobiernan estas interacciones.

Este estándar fue divulgado el 1 de Agosto de 1995 con la participación de países como Australia, Brasil, Canadá, República Checa, Dinamarca, Finlandia, Francia, Alemania, Irlanda, Italia, Japón, Corea, los Países Bajos, España, Suecia, Reino Unido, y los Estados Unidos de América.

Ha sido tal su utilidad y acogida a nivel de la industria, específicamente la industria del software, que se el estándar ISO/IEC 12207 continúa evolucionando y actualizando su propuesta, de tal forma que su última versión ha sido divulgada en el año 2008.

5.1.5.1. Enfoque

Este estándar establece un marco común para los procesos del ciclo de vida del software, con una terminología bien definida, que puede ser utilizada por la industria del software. Contiene los procesos, las actividades y las tareas que se aplican durante la adquisición de un producto software o servicio y durante el suministro, desarrollo, operación, mantenimiento y retirada de productos software.

Este estándar es aplicable a la adquisición de productos software o una parte del sistema, así como de los servicios, ya sea de forma interna o externa a la organización. Proporciona un proceso que puede ser empleado para definir, controlar y mejorar los procesos del ciclo de vida del software.
Principios

El objetivo del estándar ISO/IEC 12207 es proporcionar un conjunto de procesos definidos para facilitar la comunicación entre compradores, proveedores y otros involucrados en el ciclo de vida de un producto software.

Este estándar está enfocado tanto para las organizaciones que adquieren sistemas o productos software y servicios, como para quienes proveen, desarrollan, operan, mantienen, gestionan y llevan el control de calidad de los productos software.

Este estándar puede ser utilizado en los procesos de adquisición como soporte para el desarrollo de un acuerdo o contrato relacionado con las actividades o procesos a realizar. Ofrece una orientación para el desarrollo del contrato de adquisición.

5.1.5.2 Fases

Este estándar comprende dos grupos, el primero definido como los procesos del contexto del sistema y el segundo definido como los procesos específicos del software. Estas dos divisiones se agrupan en siete procesos agrupados como se muestra en la Figura 2-2. Cada uno de esos procesos está compuesto por actividades y tareas. Para el caso de esta tesis, se describen las actividades y tareas correspondientes al proceso de adquisición en la Tabla 2-1.

El proceso del acuerdo se clasifica en dos procesos, el proceso de la adquisición y el proceso del proveedor, cada uno con sus respectivas actividades y tareas.

5.1.6. Estándar IEEE 1062[10]

El estándar **IEEE** 1062:1998 - IEEE Recommended Practice for Software Acquisition, es un marco de referencia con la misma relevancia de modelos como SW-CMM, SA-CMM, ISO 9000, ISO/IEC 15504.

En este estándar se describe una práctica que puede ser utilizada para la adquisición de cualquier producto de software, para cualquier tipo de plataforma computacional, independiente de su tamaño y complejidad. A pesar de que este estándar está enfocado a la adquisición de productos MOST (modified off the shelf software MOTS) o FD (partially to fully outsourced FD).

5.1.6.1 Enfoque

El estándar **IEEE** 1062 define una clasificación para los productos software según el grado de libertad que tiene el usuario para definir y especificar sus

funcionalidades. Esta clasificación está compuesta por tres tipos de productos software:

COTS - Commercial-off-the-shelf-software: se refiere a un producto comercialmente disponible. Normalmente, este tipo de productos está bien definido y documentado, y su uso en escala, por un gran número de usuarios, demuestra su desempeño. El proveedor no tiene libertad para modificarlo según las necesidades de un cliente específico, ni para controlar su mantenimiento. El costo para adquirir el software es de bajo a mediano y la entrega del producto es inmediata.

MOTS - Modified-off-the-shelf-software: este tipo de productos se caracteriza porque es configurable, es decir, está elaborado pero el proveedor tiene posibilidad para modificar determinadas funcionalidades del producto software según los requisitos del cliente. El desempeño del producto se puede mostrar en aplicaciones semejantes configuradas para otros clientes. El cliente tiene un control relativo del mantenimiento del producto y de sus características de calidad. El tiempo de entrega varia de mediano a largo plazo y el coste para el cliente suele estar entre mediano y alto.

FD - Fully Developed Software: se refiere al software hecho a medida, es único, y es desarrollado para atender completamente los requerimientos de un cliente específico. Como el producto no tiene precedente, su desempeño no puede ser evaluado a priori, pero el cliente posee total control sobre sus características de calidad y mantenimiento. El costo de desarrollo para el cliente es alto y el tiempo de entrega es a largo plazo.

5.1.6.2 Principios

Busca estandarizar las fases de la adquisición de software dentro de las organizaciones, así como tener en cuenta las características de calidad necesarias durante la planificación de la adquisición y promover prácticas útiles para evaluar la capacidad que tiene el proveedor para responder a los requisitos de la organización. Con respecto al software, este estándar busca promover las prácticas útiles para evaluar y modificar el software que el proveedor está ofreciendo a la organización.

5.1.6.1. Fases

Según el estándar, el ciclo de vida de la adquisición de software representa el período de tiempo que comienza con la decisión de adquirir un producto de software y termina cuando el producto tiene su uso discontinuado. Este ciclo de vida representa un marco de referencia para la adquisición.

La estructura definida por este estándar está compuesta por fases. Cada fase está compuesta de pasos como se muestra en la Tabla 2-2.

5.1.7. Modelo CMMI-ACQ [11]

El Modelo CMMI es un conjunto de buenas prácticas que ayudan a las organizaciones a mejorar sus procesos. Fue desarrollado inicialmente por el Gobierno Estadounidense y el Instituto de Ingeniería de Software (SEI) para aplicarlos en la mejora de procesos de desarrollo de productos y servicios en todo el ciclo de vida. Luego del éxito de modelos de CMMI para organizaciones de

desarrollo, se identifica la necesidad de un modelo CMMI para el entorno de adquisición.

Un grupo de patrocinadores, entre los que se encuentra General Motors, apoyan el desarrollo de un modelo inicial para la constelación de adquisición de CMMI que pasó a llamarse CMMI – ACQ. El resultado es un modelo oficialmente aceptado tanto por el gobierno como por la industria. Tanto así, que la Oficina de Secretario de Defensa (OSD) reconoció el valor de utilizar este modelo inicial de CMMI - ACQ como una base para pilotar y desarrollar el modelo de adquisición definitivo y validarlo.

5.1.7.1 Enfoque

El Modelo CMMI – ACQ está diseñado especialmente para las organizaciones que adquieren software y servicios correlacionados. Proporciona una orientación para gestionar los proyectos relacionados con la adquisición de productos y servicios.

Se establecen unas prácticas y éstas a su vez se centran en las actividades necesarias para la contratación del proveedor, el inicio del proyecto y la concesión del contrato, así como la gestión de la adquisición de productos y servicios, por medio de un sistema de medidas, criterios de aceptación y estándares de entregables del proveedor.

Este modelo se basa en la estructura de CMMI que incorpora el concepto de constelaciones como agrupaciones de los componentes que apoyan el uso del modelo y se basa en CMMI-AM, un modulo que establece las mejores prácticas del CMMI adaptadas a la adquisición; y SA-CMM, un modelo de capacidad y madurez para organizaciones que adquieren soluciones.

5.1.7.2 Principios

CMMI para la adquisición (CMMI – ACQ) contiene dieciséis áreas de proceso categorizadas en cuatro categorías:

- Gestión de procesos,
- Gestión de proyecto,
- Soporte
- Adquisición.

La cuarta categoría incluye las siguientes áreas de proceso propias del proceso de adquisición:

- solicitud y contrato con el proveedor,
- gestión de la adquisición,
- desarrollo de los requerimientos,
- soluciones técnicas y
- validación y verificación.

Este modelo describe todas las prácticas de las áreas de procesos con una orientación y alineación con las actividades del adquirente. Para las actividades del proveedor se acopla al modelo CMMI para desarrollo (CMMI-DEV).

5.1.7.3 Fases

La estructura que tiene el modelo sigue la filosofía descrita en el punto anterior y se muestra en la Figura 2-3.

5.1.8 Modelo ESCM-CL [12]

El IT Services Qualification Center (ITSqc) liderado por la Universidad Carnegie Mellon ha desarrollado el eSourcing Capability Model for Client Organizations (eSCM-CL). Este es un modelo proporciona a las organizaciones clientes, un conjunto de mejores prácticas para evaluar y mejorar su capacidad de fomentar las relaciones con los proveedores de forma más eficaz y a su vez gestionar mejor dichas relaciones.

Este modelo permite a las organizaciones clientes tener evolución, mejora e innovación continua y establecer relaciones de confianza con sus proveedores de servicios.

El modelo eSCM-CL aborda una amplia gama de tareas de la organización cliente, que van desde el desarrollo de la estrategia de adquirir (outsourcing) de la organización, la planificación para la adquisición y la selección de proveedor de servicios. Iniciando con el establecimiento del acuerdo con proveedores de servicios, la gestión de la prestación de servicios hasta completar el acuerdo.

Este modelo ha sido propuesto porque previamente se identificaron que, los diferentes modelos de calidad carecen de marcos de trabajo orientados a conseguir exitosamente la adquisición de IT, por las organizaciones cliente.

Es un modelo de mejores prácticas que permite, a las organizaciones cliente, evolucionar, mejorar e innovar su capacidad de desarrollar relaciones fuertes, durables y de confianza con sus proveedores de servicios, a la vez que satisface las necesidades del negocio. El modelo ofrece una orientación para llevar a cabo una gestión eficaz de los servicios entregables por el proveedor de servicios.

El modelo eSCM-CL está enfocado a las organizaciones cliente y se enfoca de manera especial en establecer y mantener la relación cliente-proveedor. Es un modelo de mejores prácticas que ofrecen a la organización cliente un camino a seguir para mejorar su capacidad durante todo el ciclo de vida de la adquisición.

Este modelo tiene dos objetivos:

1) proporcionar a las organizaciones clientes un camino a seguir que ayudaría a mejorar su capacidad a lo largo del ciclo de vida de la adquisición.

2) ofrecer a las organizaciones cliente el objetivo principal de evaluar su capacidad de adquirir.

5.1.8.1 Principios

La filosofía que tiene el modelo eSCM-CL es hacer posible que las organizaciones clientes evalúen y mejoren su capacidad de fortalecer el desarrollo de relaciones con el proveedor de servicios más efectivas, llevar a cabo una mejor gestión de dichas relaciones y experimentar menos fracasos con las relaciones.

5.1.8.2 Fases

El eSCM para organizaciones cliente está compuesto por 95 prácticas que dirigen las capacidades críticas de la organización cliente, que están involucradas en la adquisición de servicios TI. Cada una de sus prácticas está distribuida a lo largo de tres dimensiones: ciclo de vida de adquisición, áreas de capacidad y niveles de capacidad. En la Tabla 2-3 se describen las áreas de capacidad que comprenden

la estructura general del modelo. La clasificación del ciclo de vida indica el número de prácticas que comprenden cada área de capacidad.

5.1.9 Information Technology: An Audit Guide for Assessing Acquisition Risks (Tecnología de la Información: Una guía de auditoría para la evaluación de los riesgos de Adquisición)

Documento de la Metodología de General Accounting Office **GAO (**Oficina General de Responsables).

- Donde se encuentra todo lo referente a la documentación y requisitos sobre los riesgos de adquisición de software.
- El mapa de la guía de Auditoría que se encuentra en el documento es el siguiente:

Fase de la Adquisición	Pasos en cada fase	Capítulo
I: Pre solicitación	Iniciar el proyecto	2,3
	Analizar Requisitos	4
	Identificar alternativas	5
	Preparar Plan Adquisición	6
	Preparar Especificaciones	4
II. Solicitud y Asignación	Mantener la Estructura del Proyecto	2,3
	Preparar Solicitud	7
	Lanzamiento de Solicitud	8
	Evaluar las propuestas	8
	Negociar con los Vendedores	8
	Seleccione Contratista	8

III. Post Solicitación	Establecer Contrato de Gestión	9
	Mostrar beneficio del contrato	9
	Evaluar y Aceptar el Sistema	10

Tabla 1: Fase de la Adquisición

Cada capítulo contiene los aspectos fundamentales que se deben tener presente en la adquisición de un software, se referencia en los siguientes ítems:

- Los objetivos de la auditoría
- La documentación requerida
- Los pasos de la auditoría
- Referencias que se necesitan

Básicamente es un "**Cómo**" hacer una gestión de riesgos, auditando cada fase del proceso de adquisición de software.

A demás incluye una serie de apéndices que complementan todos los aspectos importantes mencionados anteriormente.

GAO fue fundada en 1921 como un establecimiento del gobierno independiente del poder ejecutivo, hasta el año 2004. **GAO** es la abreviatura de Oficina General de Contabilidad de los Estados Unidos.

Con los años, **GAO** ha sido denominada "El perro guardián del Congreso" y "Mejor de los contribuyentes" amigo "para sus auditorías frecuentes e informes de investigación que han descubierto despilfarro e ineficiencia en el gobierno.

Las noticias, los medios de comunicación, la televisión a menudo resaltan el trabajo de **GAO** haciendo reportajes sobre los hallazgos, conclusiones y / o recomendaciones que aparecen en sus informes.

5.1.10 International Organization for Standarzation – ISO 9000 Normas de Sistemas de Gestión de Calidad

5.1.10.1 Introducción

La estandarización internacional es establecida para muchas tecnologías en los campos diversos tales como la tratamiento de la información y las comunicaciones, textiles, empaquetando, distribución de mercancías, de la producción energética y de la utilización, de la construcción naval, de actividades bancarias y de servicios financieros. Continuará creciendo en la importancia para todos los sectores de actividad industrial para el futuro próximo. Las razones principales son: El progreso mundial en economías de hoy del libre-mercado de la liberalización comercial cada vez más diversas de la fuente y proporciona las oportunidades para los mercados que se amplían. En el lado de la tecnología, la competencia leal necesita ser basada en las referencias comunes identificables, claramente definidas que se reconocen a partir de un país al siguiente, y a partir de una región a la otra.

Las Normas ISO 9000 son un conjunto de normas y directrices internacionales para la gestión de calidad, esta serie fue creada por comités integrados por representantes de 27 países, los cuales a su vez se encargan de revisarlas y mantenerlas actualizadas; ha sido adoptadas por más de 70 países.

Desde su publicación inicial en 1987, han obtenido una reputación global como base para el establecimiento de sistemas de gestión de calidad. Las normas de aseguramiento de calidad más modernas tienen su origen en las relaciones contractuales entre fabricantes y suministradores de algunos sectores en los que requería la mayor fiabilidad.

Los protocolos de ISO requieren que todas las normas sean revisadas al menos cada cinco años para determinar si deben mantenerse, revisarse o anularse. La versión de 1994 de las normas pertenecientes a la familia ISO 9000, fue revisada por el Comité Técnico ISO/TC 176, publicándose el 15 de diciembre del año 2000.

Existen cuatro vertientes de las normas ISO:

- **ISO 9001.** Modelo para el aseguramiento de la calidad en: diseño, desarrollo, producción, instalación y servicio.
- **ISO 9002**. Modelo para el aseguramiento de la calidad en: producción, instalación y servicio.
- **ISO 9003.** Modelo para el aseguramiento de la calidad en: inspección y ensayos finales.
- **ISO 9004.** Guías para los sistemas y la administración de la calidad.

Las normas requieren de sistemas documentados que permitan controlar los procesos que se utilizan para desarrollar y fabricar productos. Estos tipos de normas se fundamentan en la idea de que hay ciertos elementos que todo sistema de calidad debe tener bajo control, con el fin de garantizar que los productos y servicios de calidad se fabriquen en forma consistente y a tiempo.

5.1.10.2 Alcance

La revisión de las normas ISO 9001:2000 se ha basado en los Principios de Gestión de Calidad, que reflejan las mejores prácticas de gestión. Estos principios se pueden utilizar por la dirección como un marco de referencia para guiar a las organizaciones hacia la consecución de la mejora del desempeño. [19]

Principio 1- Organización orientada al cliente: Las organizaciones dependen de sus clientes y por lo tanto deberían comprender las necesidades actuales y futuras de los mismos, satisfacer sus requisitos y esforzarse en exceder sus expectativas.

Principio 2- Liderazgo: Los líderes establecen la unidad de propósito y la orientación de la dirección de la organización. Ellos deberían crear y mantener un ambiente interno, en el cual el personal pueda llegar a involucrarse totalmente en el logro de los objetivos de la organización.

Principio 3- Participación del personal: El personal, a todos los niveles, es la esencia de una organización y su total implicación posibilita que sus habilidades sean usadas para el beneficio de la organización.

Principio 4- Enfoques basados en procesos: Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso.

Principio 5- Enfoques de sistemas para la gestión: Identificar, entender y gestionar los procesos interrelacionados como un sistema contribuye a la eficacia de una organización en el logro de sus objetivos.

Principio 6- Mejora continúa: La mejora continúa en el desempeño global de la organización debería ser un objetivo permanente de ésta área.

Principio 7- Enfoque basado en hechos para la toma de decisión: Las decisiones eficaces se basan en el análisis de los datos y la información.

Principio 8- Relación mutuamente beneficiosa con el proveedor: Una organización y sus proveedores son interdependientes, y una relación mutuamente beneficiosa aumenta la capacidad de ambos para crear valor.

Figura 1: Sistemas de Gestión de Calidad- Mejora Continua

5.1.11 Control Objetives for Information and Related Technology – COBIT versión 4.1)

5.1.11.1 Introducción

COBIT es una entidad que proporciona unos principios para los administradores de procesos que se desarrollan en Tecnologías de información y que deben

responder de manera eficiente y efectiva tanto para el negocio de la organización como para su control.

Por otro lado SAC ofrece ayuda a los interventores internos en el control y la intervención de los sistemas y de la tecnología de información. Mientras COSO hace recomendaciones a la gerencia sobre cómo evaluar, divulgar, y mejorar sistemas de control que puede enriquecerse con SAS 55/78 el cual proporciona la dirección a los interventores externos con respecto al impacto del control interno en el planeamiento y la ejecución de una intervención de los estados financieros de una organización.

La importancia de que existan diferentes entidades tanto a nivel académico como organizacional que investiguen y mejoren las prácticas de control en diferentes campos, es que cada documento se centra en control interno y cada audiencia, es decir, interventores internos, gerencia, e interventores externos, dedica muchas horas y esfuerzo hacia establecer controles internos y a la evaluación de los mismos. Por lo tanto, comparar los conceptos internos del control presentados en estos documentos es de interés para los miembros de las tres audiencias.

5.1.11.2 Definición de Control

La Fundación de Auditoría y Control de sistemas de información (**ISACF** por sus siglas en inglés) desarrolló los Objetivos del Control para la Información y Tecnología relacionada (**COBIT**) al servicio de la seguridad y del control para la supervisión de las tecnologías de información y sus servicios, permite que los interventores verifiquen sus opiniones sobre control interno y que aconsejen sobre su posición ante materias tales como la seguridad y el control. La motivación primaria para proporcionar este marco es permitir el desarrollo de la política clara y

de las buenas prácticas para de la misma sobre el control a través de la industria de la tecnología.

La definición de control para **COBIT** proviene de **COSO**: “Conjunto de políticas, procedimientos, prácticas y estructura organizacional diseñadas para proporcionar un aseguramiento real para que los objetivos de negocio sean alcanzados y que los acontecimientos indeseados sean prevenidos, detectados y corregidos a tiempo.

Para COBIT el control de la tecnología es un propósito deseado, el cual debe ser alcanzado, por medio de la implementación de procesos de control en actividades directamente relacionadas con la tecnología.

En general COBIT orienta sus esfuerzos a: calidad, responsabilidad y seguridad en la información financiera.

5.1.11.3 Características

COBIT ha sido desarrollado como estándares generalmente aplicables y aceptados para mejorar las prácticas de control y seguridad de las Tecnologías de Información (TI), aportando un marco de referencia para los administradores, usuarios y auditores de tecnología.

El objetivo de esta metodología es investigar, desarrollar, publicar y divulgar Objetivos de Control de TI internacionales, actualizados a la realidad y necesidades actuales para ser usado por los Gerentes de Negocios y Auditores. Está conformado por cuatro libros:

- Resumen ejecutivo: Provee a la administración un entendimiento de los principios y conceptos claves de COBIT y el marco para el administrador esta formado por 4 dominios que a su vez estad formados por procesos, en total 34.

- Antecedentes y Marco de Referencia: Describe en detalle los 34 objetivos de control de TI, identifica los requerimientos del negocio para la información e impactos preliminares de los recursos involucrados en la TI de la organización.

- Guías de Auditoria: Contienen pasos de auditoria sugeridos correspondientes a cada uno de los 34 objetivos de control de TI, para asistir a los auditores de sistemas de información y proveer seguridad a la administración.

- Herramientas de Implementación: Contiene el conocimiento de la Administración y diagnóstico de Control de TI, FAQ, casos de estudio y presentaciones entre otras ayudas.

Alguna de las características y campos de acción de la metodología son:

CAMPO	ALCANCE
✓ Grupo Objetivo	Administradores de TI y en general, usuarios, auditores de sistemas de información.
✓ El control interno visto como	Conjunto de procesos que incluyen las políticas, procedimientos, prácticas y estructura organizacional.
✓ Objetivos Organizacionales del control interno	Efectividad y eficiencia de las operaciones. Confidencialidad, integridad y validez

	de la información. Divulgación de la información financiera confiable.
✓ Componentes o Dominios	Planeación y Organización. **Adquisición e implementación** Entrega y soporte Monitoreo
✓ Interés	Información Tecnológica
✓ Eficacia en la evaluación del control interno	Procedimiento periódico de la evaluación y procesos.
✓ Responsabilidad del sistema del control interno	Responsabilidad del Administrador

Tabla 2. Campos de acción de COBIT

5.1.11.4 Componentes

COBIT incorpora cinco componentes derivados de **COSO y SAC**.

5.1.11.4.1 Ambiente de Control:

Es un componente y parte de la actividad en sí misma. Los factores que afectan el ambiente del control incluyen la integridad y los valores éticos de la gerencia, de la capacidad del personal, del estilo de la filosofía de la gerencia y del funcionamiento, cómo se asignan la autoridad y las responsabilidades, y de la dirección proporcionada por la junta directiva.

COBIT teje las implicaciones del ambiente de control en todos los objetivos aplicables del control. Categorizar los procesos dentro del planeamiento y de la organización, de la adquisición y de la puesta en práctica, de la entrega y de la ayuda, y de la supervisión.

5.1.11.4.2 Información y sistemas de comunicación:

El interés exclusivo de COBIT, es el establecer un marco de la referencia para la seguridad y el control en tecnología de información. Define un acoplamiento claro entre los controles de sistemas de información y los objetivos de negocio.

Además, proporciona los objetivos globales validados desde el punto de vista del control para cada proceso de la tecnología de información que dé la dirección de la organización. COBIT también proporciona una herramienta para facilitar comunicaciones entre la gerencia, usuarios e interventores con respecto a controles de sistemas de información.

5.1.11.4.3 Actividades de control:

Examina los procedimientos del control concernientes al sistema de información automatizado de una entidad y los procesos que lo componen. Además clasifica los controles en 32 procesos agrupados naturalmente en cuatro dominios aplicables a cualquier ambiente del tratamiento de la información y organización.

5.1.11.4.4 Análisis de Riesgos:

Identifica un proceso dentro del ambiente de la tecnología de información como un posible generador de riesgos para el sistema. Este proceso en particular se realiza en el dominio del Planeación y de Organización, y tiene seis objetivos específicos del control asociados a él.

Trata en profundidad, varios componentes del análisis de riesgo en un ambiente de tecnología de información. Éstos incluyen el análisis de riesgos del negocio, el acercamiento de riesgos, la identificación del riesgo, la medida de riesgo, el plan de acción del riesgo y la aceptación del riesgo.

Se ocupa directamente de los tipos de riesgos de la tecnología de información, tales como tecnología, seguridad, continuidad y riesgos reguladores. Además, trata riesgos de una perspectiva global y sistema-específica.

5.1.11.4.2 Monitoreo

Incluye explícitamente la supervisión y monitoreo como componente del sistema del control interno. COBIT da la responsabilidad a la gerencia de supervisar todos los procesos de la tecnología de información y denota la necesidad de obtener aseguramiento independiente en controles. Clasifica la supervisión como dominio en línea con el ciclo de la gerencia.

5.1.11.3 Ventajas

COBIT proporciona la definición de controles y de los objetivos del control para los procesos específicos de la tecnología de información; los informes de los

problemas internos del control se asumen para estar disponibles a una variedad de fuentes para el responsable del proceso del negocio. Éstos pueden extenderse de la autovaloración del control a las revisiones externas de la intervención.

Este modelo apoya evaluaciones como punto de partida y periódicas, dependiendo de la preferencia del revisor y las necesidades de la organización. Como proporciona la dirección del modelo para los 32 objetivos de los procesos, esta dirección toma la forma sobre de 250 objetivos del control. Por lo tanto proporciona más ayudas de navegación a los usuarios, dependiendo de su perspectiva particular, ponen en ejecución para organizar y categorizar objetivos del control según COBIT, los criterios de la información o los recursos de controles existentes.

Las metodologías anteriormente mencionadas como: Information Technology: An Audit Guide for Assessing Acquisition Risks (Tecnología de la Información: Una guía de auditoría para la evaluación de los riesgos de Adquisición), International Organization for Standarzation – ISO 9000 Normas de Sistemas de Gestión de Calidad y Control Objetives For Information and Related Technology – COBIT 4.1 son las que se utilizarán como efecto de la investigación.

6. ANTECEDENTES DEL PROYECTO

6.1 MODELO DE ADQUISICIÓN DE SOFTWARE A MEDIDA PARA PEQUEÑAS Y MEDIANAS ORGANIZACIONES

El proceso de adquisición de software a medida para pequeñas y medianas organizaciones es una tarea complicada en Bolivia y en el mundo porque generalmente no se cumplen con los cronogramas de tiempo y exceden el costo del producto, la calidad del software que producen los desarrolladores en nuestro medio es difícil de probar, ya que no existen ninguna empresa de este rubro que, cuente con certificación de ISO 9001, SW-CMM, CMMI-SW u otros de acuerdo con la investigación realizada.

El modelo MODBAS (Modelo Boliviano de Adquisición de Software) permitirá a las organizaciones pequeñas y medianas que deseen adquirir software a medida llevar a cabo el proceso de manera fácil y eficiente, de acuerdo con la investigación realizada ninguna utiliza estándares para la adquisición de software como el IEEE Std. 1062, SA-CMM, CMMI Adquisition Module.

Los estándares para adquisición y desarrollo están dirigidos a grandes empresas con realidades diferentes a las de nuestro país, generalmente indican que cosas hacer para estos procesos pero no menciona el como hacer, en MODBAS toma en cuenta ambos aspectos es decir el que y el como llevar a cabo la adquisición de software por parte de estas organizaciones.

6.2 METODOLOGÍA IMPLANTADA POR LA UNIVERSIDAD JESUITA DE GUADALAJARA

Esta institución tiene como metodología para la adquisición de un software lo siguiente:

Antecedentes

- Definir las metas de la organización.
- Proponer soluciones alternativas
- Describir costos
- Determinar cuánto cuesta
- Qué resuelve

Obtención de información

- Entrevistas
- Revisar y observar las operaciones (participar en ellas).

Opciones

- Dejar el software como está
- Realizar mejoras al software existente
- Implantar un nuevo software

Para la adquisición de software interviene los siguientes factores:

1. Preparar lista de requerimientos (solicitud de propuesta)
2. Evaluar alternativas
3. Contactar a usuarios para confirmar

4. Financiamiento para adquisición
5. Negociación de contrato
6. Garantía
7. Permisos y licencias

Solicitud de propuesta

- Objetivo el software
- Propósito del software
- Deseables del software
- Cobertura del software
- Descripción detallada del producto o servicio
- Especificaciones detalladas de servicios de soporte al usuario.

Evaluación de alternativas

- Validar lo que ofrece el proveedor (credibilidad de propuesta)
- Analizar propuesta
- Costo
- Disponibilidad
- Calidad
- Soporte y mantenimiento
- Configuración
- Ambiente de software
- Documentación

Posteriormente se recomienda verificar con terceros la información sobre los productos o servicios ofrecidos por el proveedor.

Contactar a usuarios

Comentar al usuario sobre las alternativas y lo que ofrece cada una de ellas Presentarle si es posible un ejemplo o demo de las diferentes alternativas Cuestionar al usuario sobre cada alternativa Y de ser posible, tomarlo en cuenta para la decisión final.

Financiamiento

Son tres los puntos que se deben considerar para el financiamiento de la adquisición:

- Renta
- Arrendamiento
- Compra

7. DISEÑO METODOLÓGICO

7.1 TIPO DE ESTUDIO

El presente proyecto se apoya en los fundamentos de la Investigación Tecnológica" Llamada tradicionalmente "investigación aplicada y desarrollo experimental", puesto que su propósito primordial se orienta a generar espacio de reflexión sobre el proceso de Adquisición de Software, en nuestro caso en pequeñas y medianas empresas del sector privado.

Lograr crear conciencia del proceso de adquisición de Software es fundamental para este enfoque. Aquí se exige un control técnico de todos los elementos que participan en dicho proceso tecnológico, lo cual deriva en la programación de equipos sofisticados, donde la utilización de estos brinda a los participantes del proceso la oportunidad de alcanzar mediante buenas practicas la alineación de los objetivos del negocio con los objetivos de TI.

Dentro de las ventajas tecnológicas de este paradigma se encuentra el uso de la red, la cual permite el acceso a la información, el desarrollo de la colaboración, el refuerzo de las capacidades, la adquisición de información y conocimiento y el establecimiento de un puente de comunicación entre las organizaciones u organismos.

La investigación tecnológica, fortalece la vinculación de la teoría y la práctica y promueve los encuentros participativos.

La investigación aplicada se basa en concepciones epistemológicas e históricas reseñadas Tales como:

El marco clásico el cual considera que esta investigación depende de investigaciones teóricas.

El Marco de Mario Bunge el cual propone una fase intermedia entre teoría y tecnología, verdad y acción.

El Marco de los sociólogos de la ciencia defiende la investigación teórica, tiene una visión empirista del conocimiento.

El Marco de los estudios en línea, los cuales parten de una fase descriptiva, para pasar a una fase teórica, luego a una fase evaluativa y por último a una fase aplicativa.

La investigación aplicativa exige una estructura metodológica y comunicacional llamada también operaciones estandarizadas como son la descripción de la situación, la exposición del modelo teórico, la construcción del prototipo, la prueba del prototipo y la implementación del prototipo.

La investigación aplicada constituye un enlace importante entre la ciencia y la sociedad, es el punto en el que los conocimientos son revertidos a las áreas de demanda ubicadas en el entorno. La tecnología aplicada está supeditada por la Investigación cuantitativa y la cualitativa.

Esta investigación verifica que todas esas herramientas estén en pro del proceso organizacional.

7.2 MÉTODO DE ESTUDIO

El método implicado en la investigación fue de carácter **Analítico**, puesto que se inicia con la identificación de cada una de los aspectos a tener en cuenta para el proceso de adquisición de software. De esta manera tomamos lo anterior para establecer una relación en las cuales se evalúan la manera que falencias existen en dicho proceso y las consecuencias (negativas o positivas) de realizar actividades que favorezcan o no en este proceso.

7.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Breve descripción:

Para la investigación realizada se utilizaron técnicas de recolección de datos como Observación Directa, el cual tiene una gran aceptación científica, la encuesta que es una Técnica cuantitativa que consiste en una investigación realizada sobre una muestra de sujetos, representativa de un colectivo más amplio que se lleva a cabo en el contexto de la vida cotidiana, utilizando procedimientos estandarizados de interrogación con el fin de conseguir mediciones cuantitativas sobre una gran cantidad de características objetivas y subjetivas de la población, y los checklist o listas de verificación que detallan uno a uno distintos aspectos que se deben analizar, comprobar, verificar, etc.

7.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Instrumento: Encuesta realizada a medianas y pequeñas empresas del sector privado.

Propósito: Verificar el conocimiento que poseen las empresas en cuanto a la gestión del proceso de adquisición de software se refiere.

7.4.1. Desarrollo de Encuesta

Se le efectuaron a **30 empresas** pequeñas y medianas del sector privado en la ciudad de Barranquilla con el fin de obtener resultados a cerca del índice de la planeación, diseño y uso de metodologías de gestión de adquisición de software a nivel estructurado.

A continuación, se presentan los resultados por las 12 preguntas diseñadas y al final una gráfica general de lo obtenido por medio de las preguntas.

Pregunta Nº 1.

¿Existen estrategias definidas para la gestión de proyectos en la organización?	**A.** Si **B.** No	30,00% 70,00%

Tabla No 3. Análisis estadístico: Pregunta Nº 1

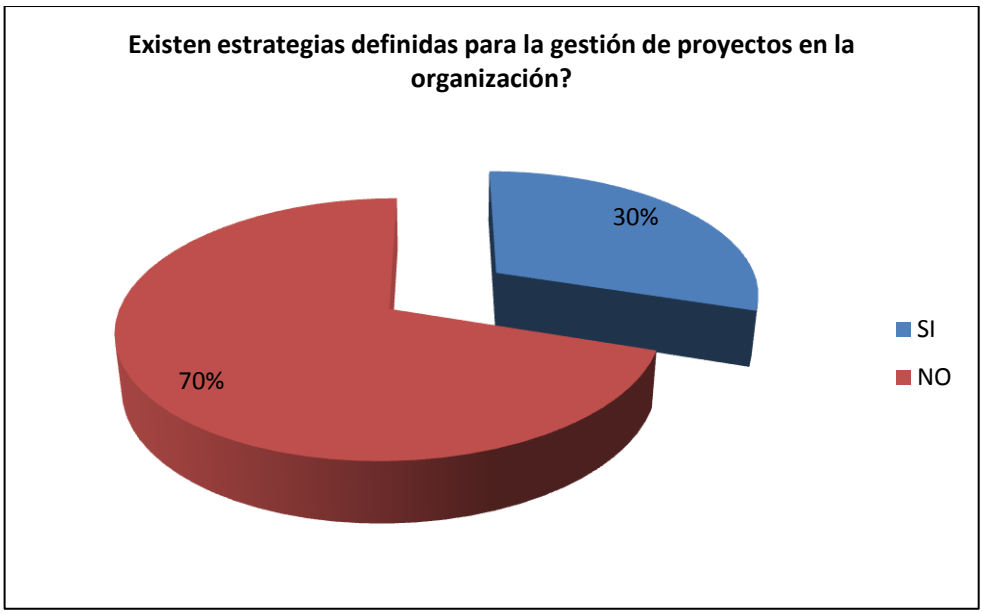

Figura 2. Análisis de Pregunta 1

Se observa que las empresas en su proceso de planificación y estrategia no tienen mucho en cuenta la definición de estrategias para la gestión de proyectos, esto nos lleva a deducir que solo el **30%** de estas empresas **SI** lo hacen, mientras que un elevado **70% NO** lo hace.

Pregunta Nº 2.

¿Se manejan indicadores de nivel de definición de las estrategias planificadas?	**A.** Si **B.** No	36,67% 63,33%

Tabla No 4. Análisis estadístico: Pregunta Nº 2

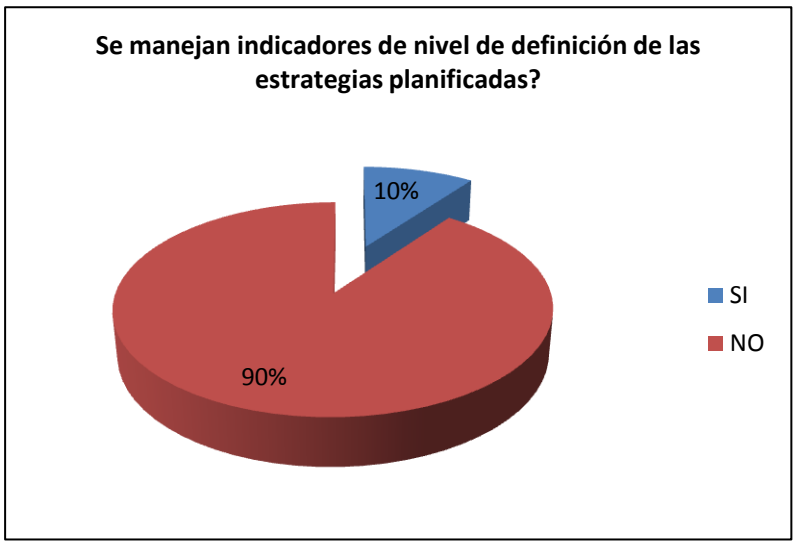

Figura 3. Análisis de la Pregunta 2

Se puede concluir de la gráfica de de las pocas estrategias definidas para la gestión de proyectos en la organización, existe un **90%** de los proyectos que **NO** se manejan o crean indicadores de de nivel de definición y existe un **10%** que **SI** realizan este tipo de planeaciones.

Pregunta Nº 3.

¿El proceso de gestión de riesgos de adquisición de software es parte de la gestión de proyectos definida?	**A.** Si **B.** No	46,67% 53,33%

Tabla No 5. Análisis estadístico: Pregunta Nº 3

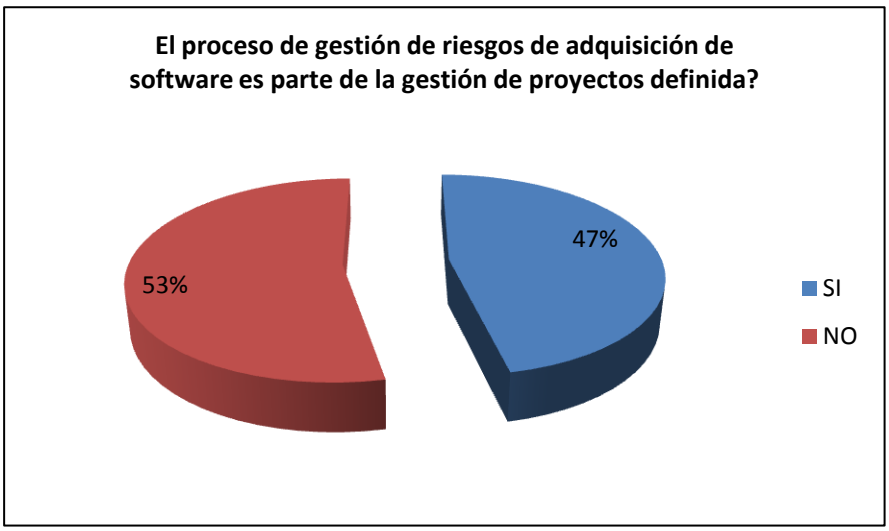

Figura 4. Análisis de la pregunta 3

Se observa que las empresas están avanzando en tomar conciencia sobre la influencia del proceso de gestión de riesgos de adquisición de software como parte de la gestión de proyectos, deduciendo esta conclusión por que existe un **47%** de empresas que **SI** lo realizan, mientras que un **53%** que **NO** lo hace.

Pregunta Nº 4.

¿Está documentado y definido el proceso de gestión y planificación de proyectos de compra de software?	**A.** Si **B.** No	43,33% 56,67%

Tabla No 6. Análisis estadístico: Pregunta Nº 4

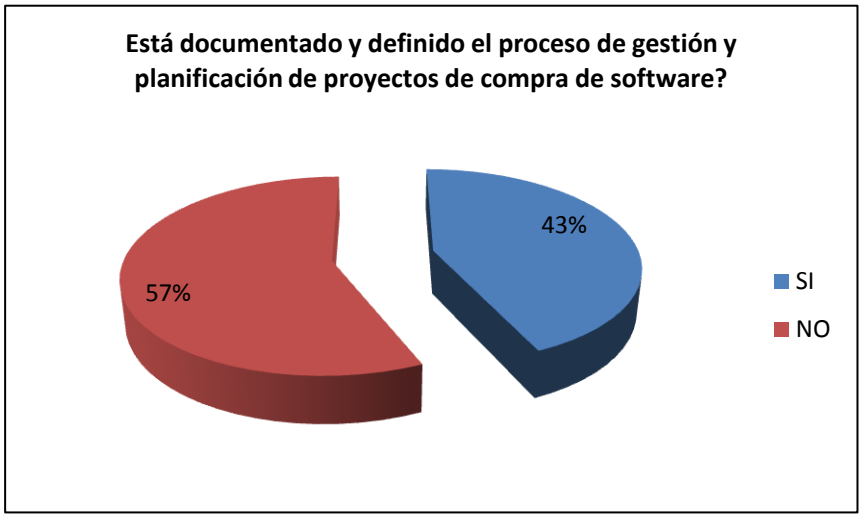

Figura 5. Análisis de la pregunta 4

La documentación y definición del proceso de gestión y planificación de de proyectos de compra de software, abarca un **43%** que lo efectúan, mientras que un **57%, NO** se tiene definido ni documentado.

Pregunta Nº 5.

¿Cuando se llevan a cabo los proyectos de compra de software se cumplen los plazos estimados?	**A.** Si **B.** No	46,67% 53,33%

Tabla No 7. Análisis estadístico: Pregunta Nº 5.

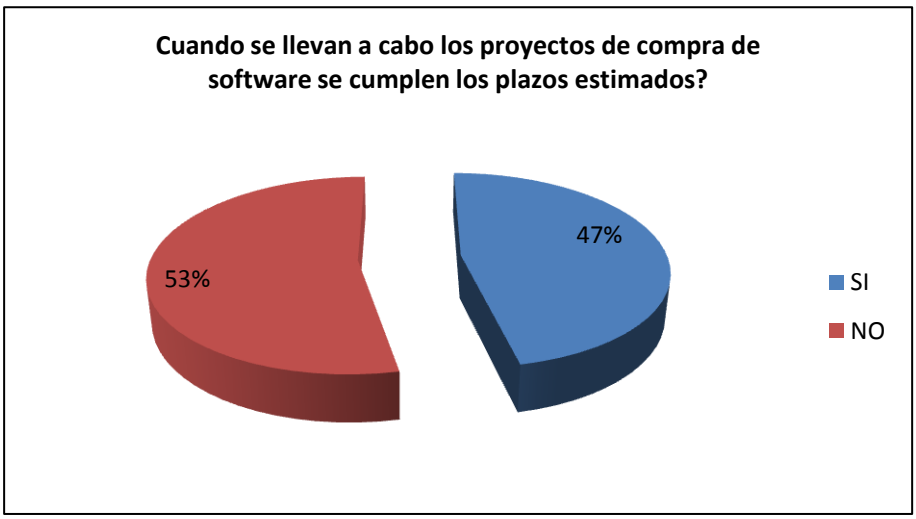

Figura 6. Análisis de la pregunta 5

Se observa que las agencias Cuando se llevan a cabo los proyectos de compra de software se cumplen los plazos estimados en un **47%** y NO lo hacen en un **53%.**

Pregunta Nº 6.

¿Los proyectos de compra son gestionados siguiendo un procedimiento establecido?	**A.** Si **B.** No	53,33% 46,67%

Tabla No 8. Análisis estadístico: Pregunta Nº 6.

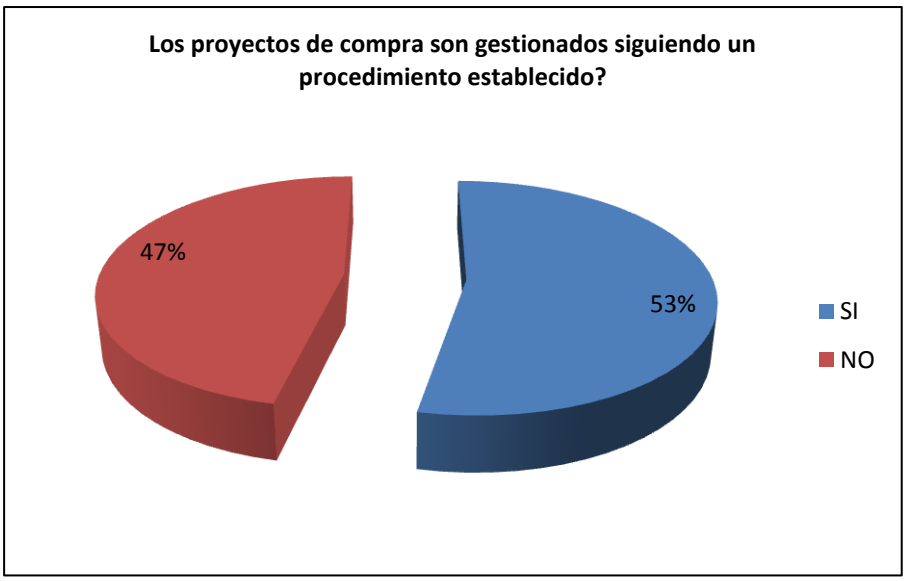

Figura 7. Análisis de la pregunta 6

Se puede deducir que las empresas que siguen una gestión para los procedimientos establecidos en los proyectos de compra de software cubren un **47%** que **NO** y un **53%** que **SI** gestiona los procedimientos.

Pregunta Nº 7.

¿Se identifican los riesgos para cada uno de los proyectos de compra de software?	**A.** Si **B.** No	46,67% 53,33%

Tabla No 9. Análisis estadístico: Pregunta Nº 7.

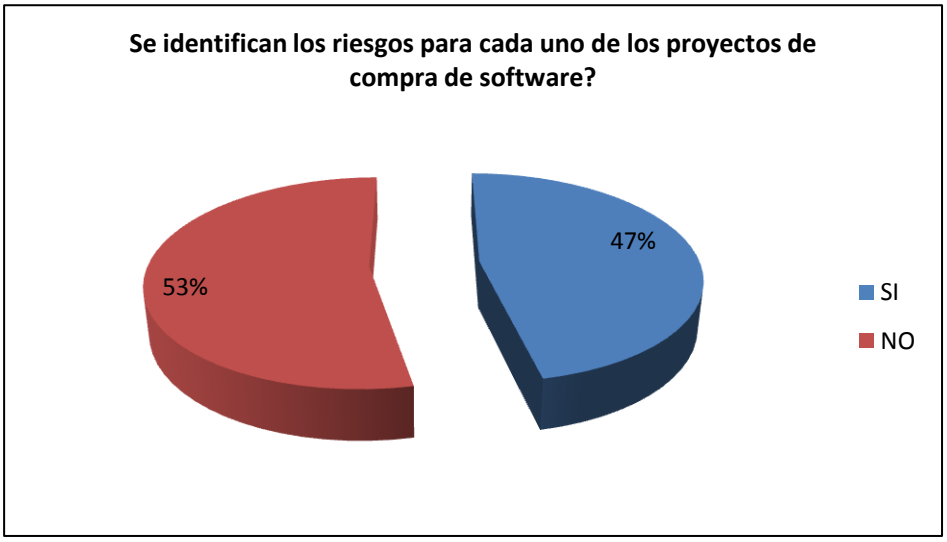

Figura 8. Análisis de la pregunta 7

En esta gráfica se observa que el **53%** de las empresas identifican los riesgos asociados a cada uno de los proyectos de compra de software, mientras que un **47% NO** lo toman en cuenta dentro de su planificación general.

Pregunta Nº 8.

¿Existe un mecanismo de establecido para analizar los riesgos de compra de software?	**A.** Si **B.** No	60,00% 40,00%

Tabla No 10. Análisis estadístico: Pregunta Nº 8.

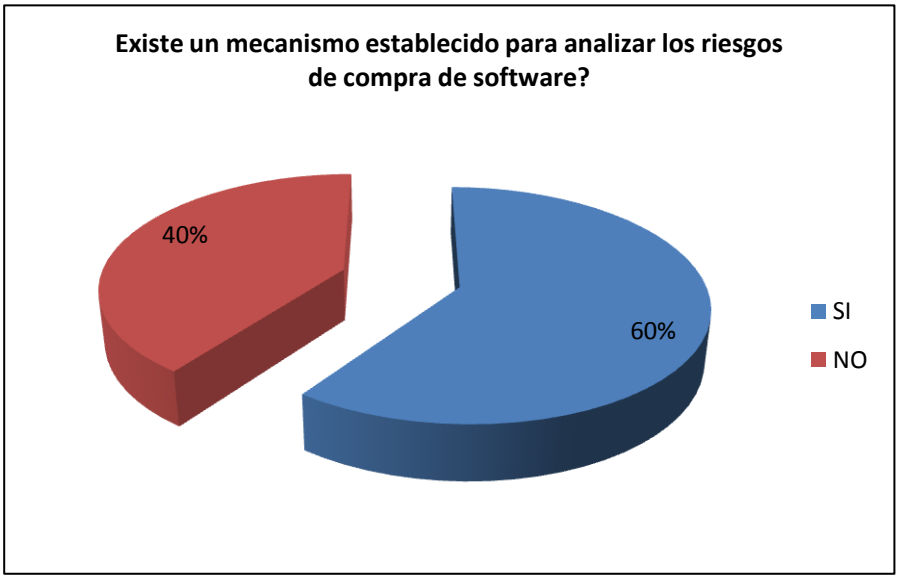

Figura 9. Análisis de la pregunta 8

Se observa en esta gráfica y deduciendo a partir de esta y la anterior, que siendo un porcentaje bajo de las empresas que identifican riesgos, existe algo muy importante, y es que gracias a esta pregunta, podemos concluir que los riesgos que si son identificados con la ayuda y /o apoyo de un mecanismo establecido para analizar los riesgos de compra de software, cuyos porcentajes están concluyendo que un **60%** los realizan de esa manera y un **40% NO**.

Pregunta Nº 9.

¿Existen planes para mitigación, supervisión y control de riesgos en los proyectos de compra de software?	**A.** Si **B.** No	36,67% 63,33%

Tabla No 11. Análisis estadístico: Pregunta Nº 9.

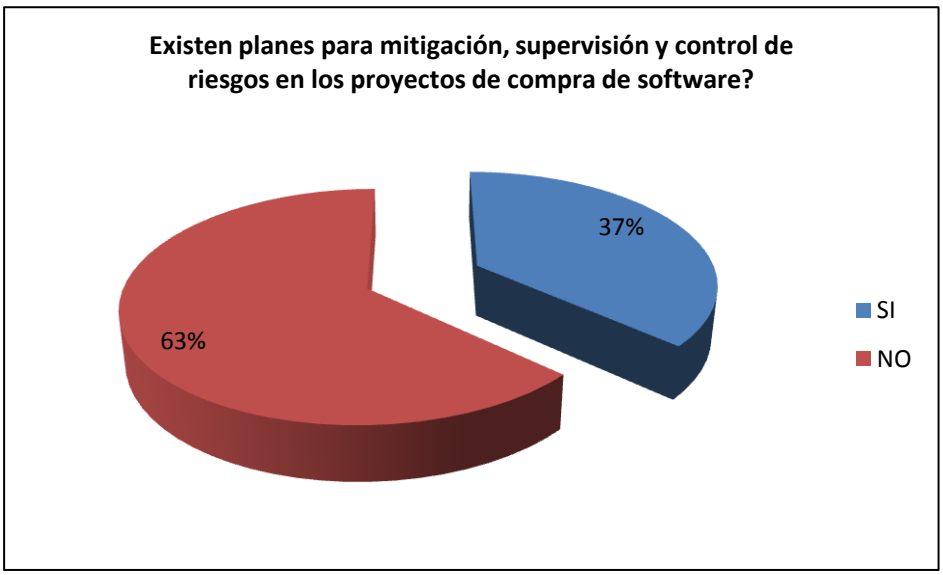

Figura 10. Análisis de la pregunta 9

Se observa que en un **37%** existen **SI** planes para mitigación, supervisión y control de riesgos en los proyectos de compra de software en cambio un **63%**, nos aseguró que **NO.**

Pregunta Nº 10.

¿Utilizaría un modelo que ayude a definir los procesos de gestión de proyectos de compra de software?	**A.** Si **B.** No	63,33% 36,67%

Tabla No 12. Análisis estadístico: Pregunta Nº 10.

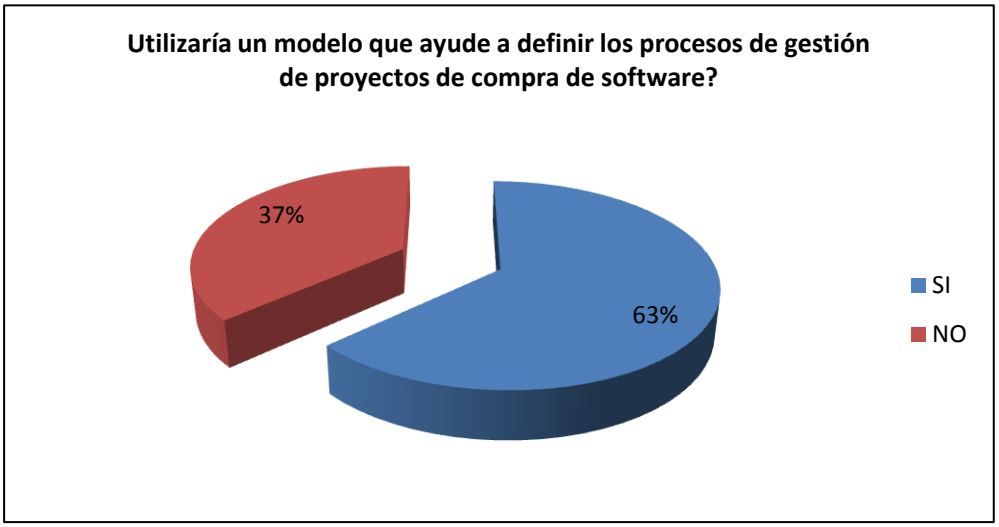

Figura 11. Análisis de la pregunta 10

Se observa en esta gráfica, lo que para muchas empresas puede representar una necesidad, otros una oportunidad, como a otros un despertar a lo verdaderamente importante, esto es a la utilización de un modelo que ayude a definir los procesos de gestión de proyectos de compra de software, esto se ve reflejado en que un **63%**, desea utilizar uno que no conocían, y un **37%**, que no querían invertir en este tipo de soluciones al igual, otros que **NO** querían cambiar su forma de hacer dicho proceso.

Pregunta Nº 11.

¿Estaría dispuesto a implementar otra metodología para el proceso de gestión de riesgo en un proyecto de compra de software?	**A.** Si **B.** No	50,00% 50,00%

Tabla No 13. Análisis estadístico: Pregunta Nº 11.

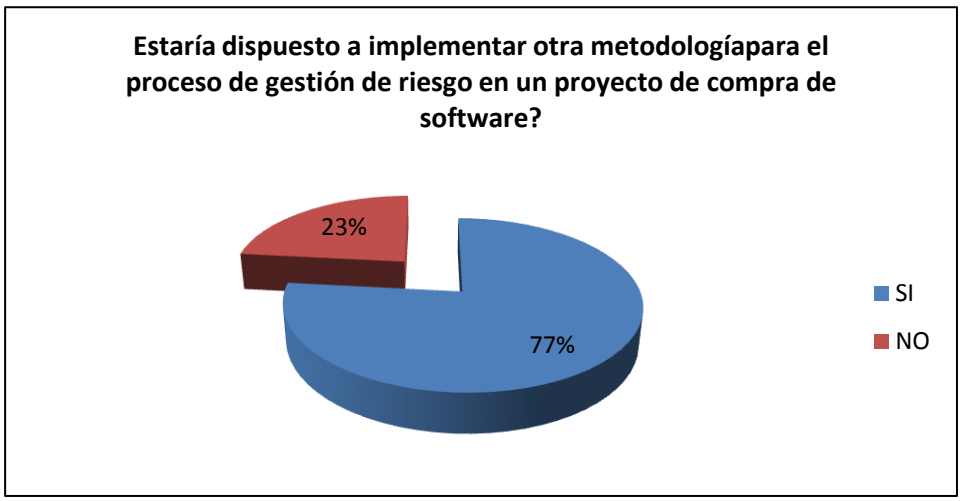

Figura 12. Análisis de la pregunta 11

Simplemente se puede decir la gran parte estarían dispuestos a implementar otra metodología para el proceso de gestión de riesgo en un proyecto de compra de software. O sea, **23%** que **SI** y **73%** que **NO**.

Pregunta Nº 12.

¿Los resultados de la metodología de gestión de riesgos serían tenidos en cuenta durante el desarrollo de proyectos de compra?	**A.** Si **B.** No	36,67% 63,33%

Tabla No 14. Análisis estadístico: Pregunta Nº 12.

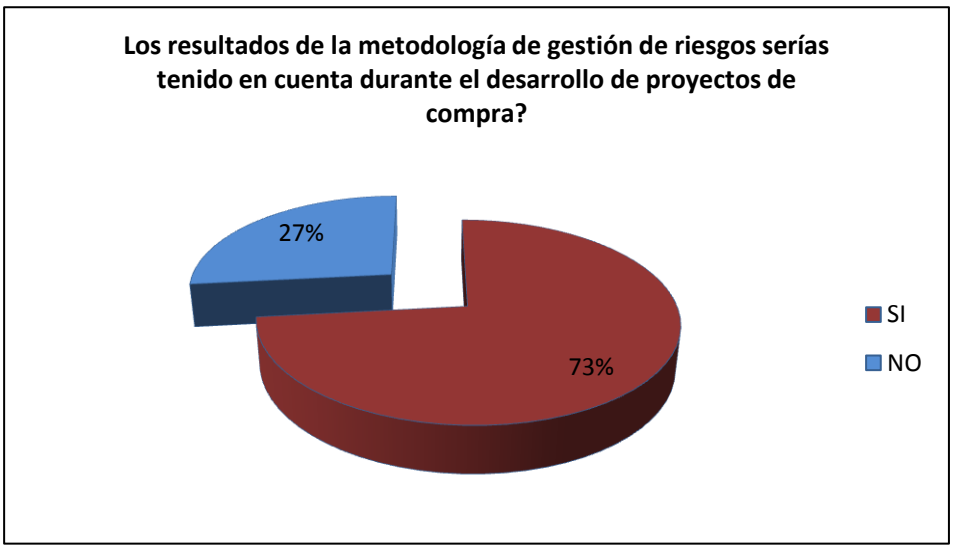

Figura 13. Análisis de la pregunta 12

Se puede concluir a partir de esa gráfica que los resultados de la metodología de gestión de riesgos serías tenido en cuenta durante el desarrollo de proyectos de compra un **73%** dice que **SI**, en cambio un **27%** dice que **NO**, porque solo lo utilizaría cuando vengan los auditores y eso es oficio de ellos.

Por último, podemos concluir con la siguiente gráfica para revisar los resultados totales:

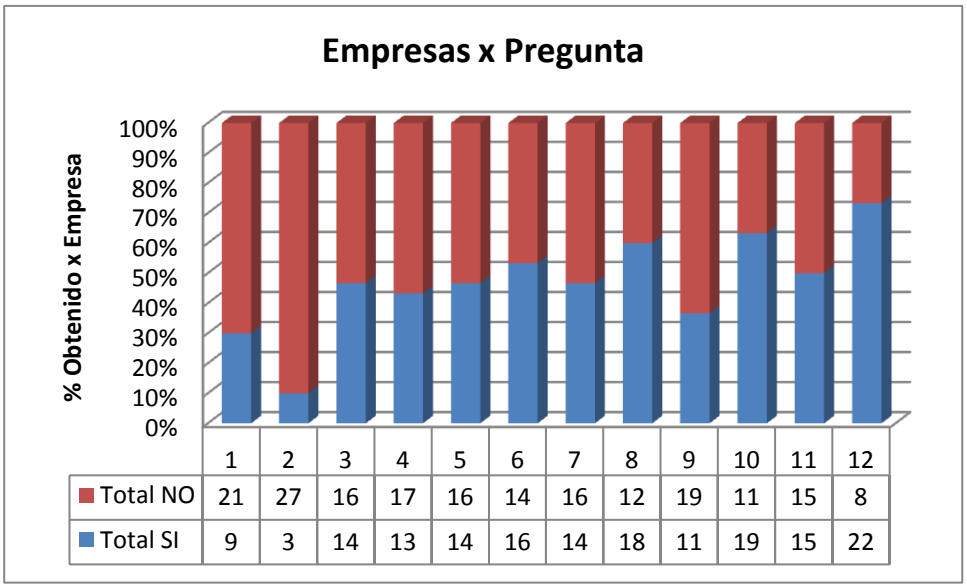

Figura 14: Conclusión del proceso de Encuesta

Concluyendo que un **46.67%** está de acuerdo con la ejecución de las mejores prácticas en la planeación y en el desarrollo de un plan de adquisición de software, y un **53.33%** que dice lo contrario por razones diferentes, unos por dinero, otros porque consideran que el empleado les ha funcionado durante todo el tiempo de ejecución.

7.5 POBLACIÓN DE ESTUDIO

Tomamos como población estudio a las Empresas pequeñas y medianas de la ciudad de Barranquilla.

7.6 MUESTRA

Se tomo una muestra representativa de 30 empresas de la ciudad de barranquilla.
Fecha de aplicación: Septiembre 13 al 17 de 2010.

8. PLAN DE TRABAJO

Esa investigación incentiva el uso de las metodologías de Adquisición de software. Recordemos que es una guía metodológica no una nueva metodología, debido a que no se propone una nueva teoría para hacer las cosas, simplemente se trata de tomar puntos claves de diferentes metodologías, analizar su viabilidad, aplicabilidad en el entorno y cultura organizacional para luego documentarla.

Se establecerán un conjunto de criterios para comparar metodologías de Adquisición de software: **Information Technology: An Audit Guide for Assessing Acquisition Risks** (Tecnología de la Información: Una guía de auditoría para la evaluación de los riesgos de Adquisición), Control Objetives for Information and Related Technology – **COBIT 4.1**) e **ISO** (International Organization for Standarization - Organización Internacional de Estandarización, y en base a estas lograr una guía de apoyo a las organizaciones para combatir uno de los inconvenientes más críticos por los que pasan las empresas hoy día.

Durante la investigación, se revisarán y ratificarán cada uno de estos criterios. Finalmente, se identificarán las ventajas de aplicarlo en un proceso de Adquisición de Software. Todo lo anterior como herramientas para garantizar características de calidad en selección, adquisición e implementación de software.

Para la realización de este trabajo, se proponen a ser analizadas y tomar puntos claves, 3 metodologías: "**GAO**" (United States General Accounting Office – Information Management and Technology Division), "**ISO**" (International Organization for Standardization) y" COBIT" (Control Objectives for Information Systems and related Technology), esperando que éstas sean flexibles y adaptables a la taxonomía y cultura organizacional.

No se pretende ser exhaustivo en esta revisión bibliográfica, sino tomar como referencia una de ellas y complementar en aquellas áreas donde haya falencias con las otras metodologías. Para luego emitir una guía metodológica que cubra prácticamente todos los ítems que se deben tener en cuenta a la hora de someter a una organización a un proceso de adquisición de software.

Luego de identificar debilidades y fortalezas a la hora de hacer la adquisición de un producto, generar las recomendaciones. Por último y con base a toda la información antes citada, se creará la Guía Metodológica para la adquisición de software para organizaciones de tamaño mediana y pequeña.

9. ANALISIS DE RIESGOS PARA EL PROCESO DE ADQUISICION

9.1 ¿QUÉ ES UN ANÁLISIS DE RIESGOS?

La información de una organización, tanto a nivel del negocio como la del campo tecnológico, se ha convertido en uno de los activos más valiosos de la organización.

Por lo anterior se requieren actividades y procesos efectivos para la administración de riesgos que puedan llegar hacerse realidad y afectar el patrimonio del a empresa; no basta con proteger los activos informáticos (hardware, software, infraestructura de redes, etc.), sino también a la organización como tal.

El control de los riesgos no solamente debe verse como una función técnica del área de informática sino como una función esencial de la administración de la empresa.

Todo sistema de información, procedimiento o actividad tiene un comportamiento similar a la de un ser vivo, por lo anterior podemos reconocer, cómo se nombra en capítulos anteriores el ciclo de vida del producto; para ésta sección se tomará el ciclo de vida de los sistemas de información:

- **Iniciación:** Detección de necesidades**.**
- **Desarrollo/adquisición:** Diseño del sistema, comprado, programado, desarrollado o construido según las necesidades encontradas.
- Implementación: El sistema se aprueba e instala.
- **Operación/mantenimiento:** Puesta en producción del sistema. Se inicia una etapa de monitoreo constante para detectar fallas y realizar modificaciones (compra, cambios, procedimientos, ajustes).

- **Destrucción:** Fin del sistema, invalidación de los datos y equipos. Obsolescencia del sistema.

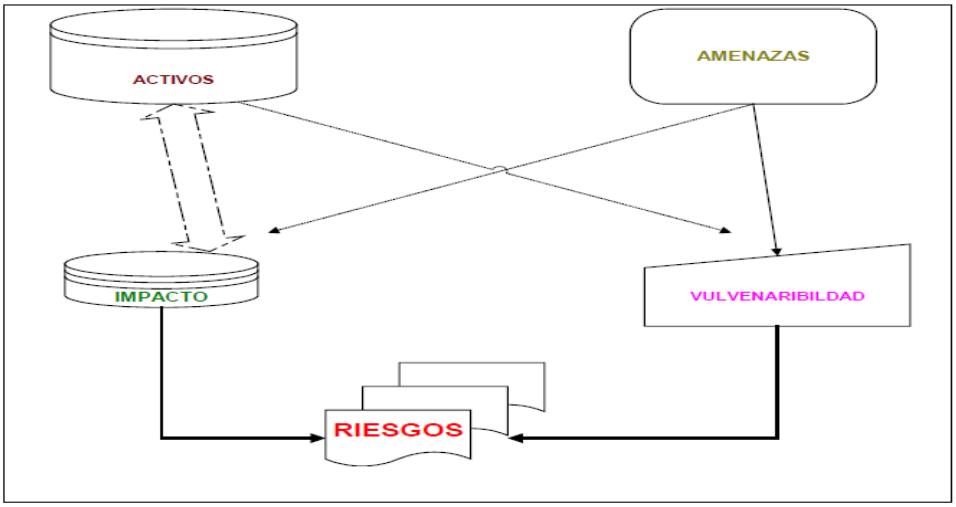

Figura 15. Elementos de conformación del mapa de exposición de la organización

Para poder llevar a la organización a un nivel aceptable de riesgos, debe realizarse un plan de mitigación de los mismos. Este plan tiene por objetivo prevenir, limitar, detectar y responder ante las vulnerabilidades:

- **Prevenir:** Eliminar la amenaza quitando la o falla o vulnerabilidad.
- **Limitar:** Implantar controles que restringen el impacto de una amenaza.
- **Detectar y responder:** Detectar la ocurrencia de una amenaza y tomar acción.

Para encontrar los controles adecuados para llevar a cabo y medir el plan de mitigación, se puede hacer un análisis de éstos por diferentes enfoques:

- Controles extraídos de políticas y guías de seguridad, procedimientos de operación de los sistemas, especificaciones de seguridad, estándares y buenas prácticas.

- Controles técnicos: Preventivos (control de acceso, antivirus, autenticaciones, encriptación, etc.), Detectivos (logs, ids) y Correctivos (prueba caja negra o blanca).
- Controles operacionales (personal, seguridad, física, etc.): Preventivos (entrenamiento, planes de contingencia y de recuperación, investigaciones), Detectivos (revisiones de seguridad y auditorias) y Correctivos (pruebas de seguridad).
- Controles administrativos: Revisión de auditorias, evaluación de riegos, reglas de comportamiento.

Luego para implementarlos, se clasifican en:

- Controles Técnicos: apoyo, prevención, detectar y recuperar.
    - Controles Administrativos: segregación de tareas y creación de políticas.
    - Controles Operacionales: seguridad física y de acceso.

9.2 ¿PARA QUÉ SIRVE?

Contar con una análisis de riesgos actualizado de la empresa, permite balancear los costos operacionales y económicos de los controles con la efectividad de los mismos. Además es necesario para mantener los valores y controles necesarios sobre los diferentes aspectos y campos que conforma la organización: nivel del servicio, imagen, competitividad, rentabilidad, permanencia, cumplimiento de la legalidad, reducción de costos, entre otros.

Adicional a los factores anteriores el análisis y gestión de riesgos juega un papel vital en el derecho y obligación de preservar la confidencialidad y privacidad de los datos, tanto de las personas que trabajan para la empresa, como aquellos que

forman el activo de la organización. Hay que sumar a esto, la protección de los miembros de la organización.

9.3 ¿CÓMO REALIZAR UN ANÁLISIS DE RIESGOS?

En la actualidad se puede encontrar variedad de bibliografía acerca de metodologías sobre la administración de riesgos; para el análisis y gestión de riesgos se pueden clasificar las metodologías existentes en: [17]

- De uso libre: Aquellas elaboradas y patrocinadas por las administraciones públicas de diferentes nacionalidades.
- Privadas: Desarrolladas por empresas consultoras para su propio uso.
- Orientadas a escenarios: Procedimientos genéricos y propios tanto del sistema de información como de la época.
- Utilización como Guía y Patrón de calidad para seguir y realizar consultorías especificas.

Como ejemplo de Metodologías libres tenemos una desarrollada por el Consejo Superior de Informática para uso en Administraciones Públicas, Magerit que se basa en un submodelo de eventos donde calcula los riesgos, las funciones y los mecanismos para salvaguardar los bienes informáticos.

Para tal fin estudia los riesgos que soporta un sistema de información y el entorno asociado con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. Recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

Para realizar un análisis de riesgos e iniciar su gestión es conveniente tener en cuenta los objetivos que guiarán la labor, sea cualquiera de las metodologías existentes a usar:

- Identificar los riegos que afecten a un sistema de información.
- Recomendar y desarrollar medidas y técnicas que prevengan impidan o controlen los riesgos identificados.
- Auditar el grado de seguridad de los sistemas y adaptar los mecanismos de controles existentes y necesarios para salvaguardar los bienes.

9.4 ANÁLISIS DE RIESGOS EN EL PROCESO DE ADQUISICIÓN DE SOFTWARE

En el momento de realizar el análisis de riesgos para el proceso, se debe tener en cuenta los roles que intervienen en la adquisición de software:

- Directivas: Autorizan la compra de software, realizan un balance costo-beneficio.
- Responsables del sistema o la información: Responsable del software, capacitación a terceros, administrador de riegos en la efectividad general de la aplicación.
- Oficiales de seguridad: Normalmente es un grupo independiente dentro de la empresa, que tiene como misión ser el responsable de la seguridad informática de los sistemas (hardware, software y datos). Debe seleccionar los controles apropiados para la adquisición e implementación de un sistema de información o software. Tiene voz y voto en la elección de los productos.
- Administrador del sistema: Monitorea el sistema luego de realizar modificaciones. Estar al tanto de posibles problemas que tengan algún tipo de incidencia o impacto en el sistema y por ende en la organización.
- Usuarios finales: Quienes utilizaran los sistemas de información o software según las políticas establecidas y la capacitación para las mismas.

Para el caso de análisis de riegos para el proceso la adquisición de software en, se utilizará la Metodología Magerit. Dicha metodología está compuesta de los siguientes pasos:

- Definición del escenario: Se define el contexto de tecnología donde se trabajará y que se quiere analizar.
- Inventario de Activos: Se listan los recursos del sistema de información o relacionados con el contexto, necesarios para que la organización funcione correctamente.
- Inventario de Amenazas: Se identifican las amenazas que puede tener el sistema.
- Inventario de Vulnerabilidades: Se listan las relaciones emergentes entre un activo y una amenaza.
- Análisis del Impacto: Se hace un inventario de las posibles consecuencias de materializarse una amenaza.
- Inventario y análisis de Riesgos: Se identifican los riesgos relacionados con el sistema y su correcto funcionamiento.
- Calculo del Riesgo: Es el coste acumulado durante un periodo de los riesgos.
- Salvaguardas: Acciones preventiva, correctivas y mitigadoras que reducen el riesgo.

10. TÉCNICAS BÁSICAS PARA IDENTIFICACIÓN DE RIESGOS

La selección de las técnicas de identificación de riesgos se ha hecho utilizando el método MSSS, al igual que los demás análisis presentados en este capítulo. Es decir, utilizando las siguientes actividades:

10.1 DEFINIR CRITERIOS PARA SELECCIONAR LAS TÉCNICAS DE IDENTIFICACIÓN DE RIESGOS

Se establecieron los siguientes criterios para seleccionar estas técnicas:

a) todas las técnicas referenciadas dentro de modelos, métodos o estándares que relacionen la gestión de riesgos.
b) aquellas técnicas que tienen información disponible.

10.2 SELECCIONAR TÉCNICAS DE IDENTIFICACIÓN DE RIESGOS

Utilizando los criterios antes mencionados se seleccionaron las siguientes técnicas:

- Entrevistas con los Implicados
- Tormenta de ideas o Brainstorming
- Método Delphi
- Técnica de Grupo Nominal (NGT)
- Crawford slip
- Método basado en analogías
- Listas de chequeo, formatos o plantillas

10.2.1 Entrevistas con los Implicados

Es una técnica utilizada para investigar asuntos relacionados con dudas o problemas de un proyecto. Implica visitas al lugar donde se encuentran o se establece la reunión con los implicados en el proyecto que participaran en las entrevistas [58].

10.2.1.1 Ventajas y Desventajas

Ventajas	Desventajas
Se involucran expertos y personal clave para el proyecto y la organización.	Se requiere expertos en el ámbito de aplicación para el éxito de la técnica.
Cuestionarios especializados en el ámbito de aplicación de la técnica.	La efectividad de la técnica depende en gran medida del buen diseño y planteamiento de los cuestionarios
Estimula el trabajo en equipo	

Tabla 15: ventajas y desventajas de las entrevistas con los implicados

10.2.1.2 Proceso

Figura 16. Proceso para llevar a cabo las entrevistas

10.2.2 Tormenta de Ideas o Brainstorming

El método tormenta de ideas o brainstorming se utiliza frecuentemente por las organizaciones con el objetivo de generar ideas y resolver problemas. Este método se considera muy útil para el intercambio y generación de ideas.

10.2.2.1 Ventajas y Desventajas

Ventajas	Desventajas
Equipo de personas disponible	Es recomendable que dicho equipo esté compuesto por personas con experiencia en el ámbito en el que se desarrollen los riesgos.
Estimula la libre expresión de las ideas (riesgos). Esto permite abarcar gran cantidad de riesgos.	Se deben contemplar todas las ideas (riesgos) de partida. Esto genera una gran cantidad de posibles ideas que necesariamente son riesgos y que aún así deberán analizarse inicialmente.
Es un método muy creativo y sinérgico	Si este método no se ejecuta de forma adecuada y bien coordinada, puede generar caos.
Estimula el trabajo en equipo	

Tabla 16: Ventajas Y Desventajas De Brainstorming

10.2.2.2 Proceso

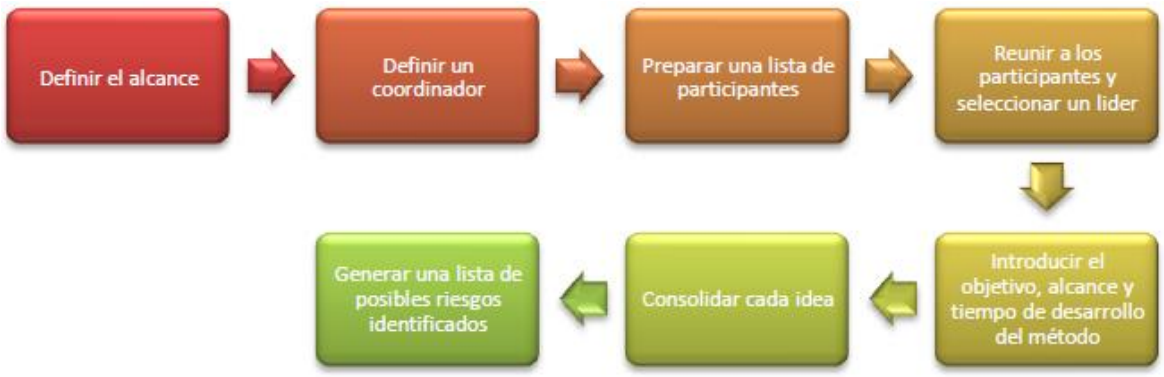

Figura 17: actividades básicas para desarrollar este método

10.2.3 Método DELPHI

Es utilizado en diferentes ámbitos por su flexibilidad y la amplia aplicabilidad que lo caracteriza. Es considerado como una técnica versátil. Es un método estructurado

para comunicación de grupos, generalmente se utiliza para permitir la comunicación eficaz de un grupo de personas que necesitan abordar un problema complejo.

10.2.3.1 Ventajas y Desventajas

Ventajas	Desventajas
Está basado en entrevistas	Requiere un diseño de entrevistas avanzado. Debe hacerse un trabajo especializado.
Las entrevistas son anónimas	No existe contacto con las personas que participan, por lo tanto no se puede motivar para obtener respuestas.
Es recomendado cuando existen conflictos y no se puede realizar una técnica como la tormenta de ideas.	No se puede controlar el tiempo que se invertirá en el proceso de desarrollo del método.

Tabla 17: Ventajas Y Desventajas De Delphi

10.2.3.2 Proceso

Figura 18. Proceso Para Desarrollar El Método Delphi

10.2.4 TÉCNICA DE GRUPO NOMINAL (NGT)

El método NGT fue desarrollado en 1968. Se genera esta técnica a raíz de estudios psicosociales, ciencias judiciales y de trabajo social. Está técnica inicia con el establecimiento de un grupo, generalmente de siete a diez personas, quienes durante unos minutos escriben sus apreciaciones respecto al problema que se aborda. Cada integrante del grupo presenta de forma breve sus ideas. Dichas ideas se registran en una pizarra, a la vista de todo el grupo. Hasta este momento no se realiza ningún tipo de debate ni discusión. Cuando se han terminado de exponer y de registrar las ideas ante todo el grupo, se discuten y debaten cada una de ellas. La técnica termina con la evaluación de los riesgos más importantes, según un rango establecido de valoración [62].

10.2.4.1 Ventajas y Desventajas

A continuación se presenta en la Tabla 2-16 las ventajas y desventajas de esta técnica.

Ventajas	Desventajas
Permite mezclar el trabajo individual con el trabajo en equipo.	Técnica de tormenta de ideas, pero de forma individual.
Existe más control de tiempo y de discusión que con la tormenta de ideas. Se controla el caos que se puede presentar con la tormenta de ideas.	No fomenta el trabajo en equipo.

Tabla 18: Ventajas y Desventajas de la Técnica de Grupo Nominal (NGT)

10.2.4.2 Proceso

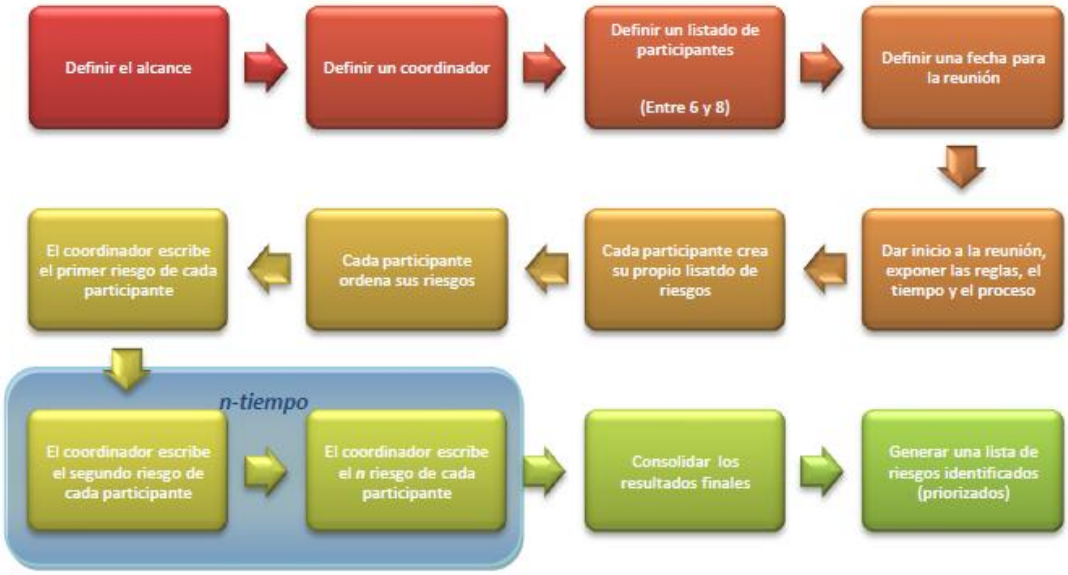

Figura 19: Proceso De La Técnica Ngt

10.2.5 Crawford Slip

Este es un método sencillo, diseñado para recoger ideas. Fue desarrollado en la década de 1920 por Mrs. Crawford con el fin de generar ideas en grupos grandes (más de 5000 personas, aunque el método es fácil de manejar con grupos de entre 50 y 200 personas).

Se considera como una variante del método de ideas escritas (BrainWriten) y su principal característica es su gran eficiencia para la recolección de ideas de muchas personas, cuando se trata de generación de ideas en grandes auditorios.

10.2.5.1 Ventajas y Desventajas

Ventajas	Desventajas
Permite identificar muchos riesgos en un corto periodo de tiempo.	Es una variación de la tormenta de ideas, pero de forma individual.
Se desarrolla de forma sencilla, utilizando un trozo de papel o un post-it.	No fomenta el trabajo en equipo.
Permite consolidar a un gran grupo de personas de forma fácil.	La información que refleja, depende del tiempo que se invierta en el desarrollo del método.

Tabla 19: Ventajas Y Desventajas Del Método Crawford Slip

10.2.5.2 Proceso

Figura 20: Proceso para desarrollar el método CRAWFORD SLIP

10.2.6 Método Basado en Analogías

Tal como su nombre lo indica, este método se basa en la comparación de dos escenarios idénticos. Es necesario tener como base algún tipo de antecedentes. Deben existir referencias para poder generar un listado de riesgos. Sin embargo, la información previa, los antecedentes y experiencia deben estar ajustados a las condiciones o el escenario actual, de lo contrario este método no puede ajustarse a las condiciones reales actuales.

10.2.6.1 Ventajas y Desventajas

Ventajas	Desventajas
Basado en antecedentes y experiencia previa.	Es indispensable que la información previa, la experiencia y los antecedentes estén ajustados al escenario en el que se desea aplicar el método.
El punto de referencia que se requiere es la experiencia con otras situaciones idénticas, por lo que la información de partida es real.	
Permite consolidar a un gran grupo de personas de forma fácil.	

Tabla 20: Ventajas Y Desventajas Del Método Basado En Analogías

10.2.6.2 Proceso

Figura 21: Proceso de desarrollo del método basado en analogías

10.2.7 Listas de Chequeo, Formatos o Plantillas

La recopilación de información a partir de la experiencia previa de otros proyectos permite la utilización de plantillas, formatos o listas de chequeo. Estas tres opciones se pueden utilizar cuando existe en la organización los datos históricos de proyectos anteriores. Estas opciones de identificación de riesgos están generadas bajo la premisa de que los nuevos proyectos nunca tienen un conjunto de riesgos del todo nuevo, sino que los nuevos proyectos deben refinar un listado de riesgos preestablecido. Estas opciones para identificar riesgos, generalmente son utilizadas a partir de una estructura de desglose de riesgos (WBS de riesgos).

10.2.8 Síntesis de Información

A continuación se presenta una comparación de las características más relevantes que abarcan esta tesis para comparar las técnicas de identificación de riesgos analizadas. Esto permite determinar cuáles, de dichas características, aborda cada una de las técnicas. Los resultados se muestran en la Tabla 2-19.

Técnica / Características	Entre vistas	Brainstorming	Delphi	NGT	Crawford slip	Analogías	Lista chequeo
Facilidad de utilización por persona involucrado en el proyecto	✓	✓		✓	✓	✓	✓
Implementación ágil	✓						✓
Control del tiempo del proceso de identificación de riesgos	✓						
Generación fácil y rápida de riesgos más importantes para el proyecto					✓		✓
Generación de priorización inicial de riesgos				✓			

Tabla 21: Comparativa De Características De Las Técnicas De Identificación De Riesgos

El estudio de las técnicas de identificación de riesgos hasta ahora expuestas, permite determinar que es necesario diseñar una técnica que apoye el proceso de identificar los riesgos. De las técnicas analizadas ninguna cumple con las características más importantes que se consideran para facilitar la identificación de riesgos y de esta forma garantizar un buen proceso de gestión de riesgos.

Este diseño debe estar orientado de forma especial para cubrir las necesidades más importantes para los pequeños entornos. Esas necesidades están centradas en las características analizadas en la Tabla 2-19. Es decir, la facilidad y agilidad en la utilización de la técnica, así como el control del tiempo para la aplicación de la misma y su facilidad en la generación de los riesgos más importantes del proyecto.
A continuación se presentan las conclusiones preliminares de este capítulo y se presentan los principales puntos a atacar en esta tesis.

10.3 DEFINIR LOS ASPECTOS A ANALIZAR DE CADA UNO DE LOS MÉTODOS

El análisis de las técnicas seleccionadas se lleva a cabo por medio del estudio de los siguientes aspectos:

Ventajas y desventajas de la técnica.
Proceso que se recomienda para la aplicación de la técnica.

10.4 IDENTIFICAR CARACTERÍSTICAS DE LAS TÉCNICAS A ANALIZAR

Las características que se van a analizar se han definido según el interés del estudio. El interés de esta tesis está principalmente enfocado en la gestión de

riesgos dentro del ámbito de la adquisición de software, pero teniendo en cuenta que la gestión de riesgos es un proceso complejo y que el éxito de este proceso está centrado principalmente en la fase de identificación de riesgos se analizará la facilidad y completitud que cada técnica de identificación de riesgos ofrece.

10.5 ESTABLECER EL OBJETIVO DEL ANÁLISIS

Este análisis se lleva a cabo con el fin de establecer cuáles de las técnicas de identificación de riesgos se adaptan a las necesidades del proceso de gestión de riesgos en el ámbito de la adquisición de software. Específicamente este análisis busca determinar las técnicas en las que se puede enfocar la propuesta que se realizará en esta tesis. Por lo tanto el objetivo de este análisis es determinar las características que se pueden incluir en la propuesta, analizando las diferentes técnicas seleccionadas desde el punto de vista de los pequeños entornos.

10.6 DEFINIR LA ESTRUCTURA PARA PRESENTAR EL ANÁLISIS REALIZADO

La estructura por medio de la cual se presentara el análisis realizado está determinada por los aspectos a analizar que se definieron antes. A continuación se presenta cada uno de los métodos de gestión de riesgos seleccionados por medio de la descripción de:

- Ventajas y desventajas de la técnica.
- Proceso que se recomienda para la aplicación de la técnica.

10.7 SINTETIZAR INFORMACIÓN

Un resumen con los hallazgos del análisis realizado se presenta al finalizar la descripción de cada una de las técnicas de identificación de riesgos. A continuación se presentan las técnicas.

11. GUÍA METODOLOGIA

11.1 ADMINISTRACIÓN Y SOPORTE AL USUARIO

Este capítulo se centra en los niveles de compromiso y apoyo para proyectos de adquisición para la alta dirección y los usuarios, dos stakeholders principales en el proceso de adquisición.

Los altos directivos son los que tienen en general la responsabilidad por motivos estratégicos, incluyendo información relacionada con los objetivos.

Los usuarios son los que en realidad operan los recursos de información de la empresa e incluyen a la dirección para establecer políticas institucionales y para los programas apoyados por la adquisición.

La participación y el apoyo de la gerencia a lo largo de un proceso de adquisición son esenciales para el éxito.

La Gerencia debe prever los objetivos de la adquisición, definir los objetivos estratégicos y supervisar los proyectos que implementan la visión general. Uno o más altos directivos deben actuar como patrocinadores o sponsors del sistema, con autoridad suficiente para garantizar que los recursos aplicables se encuentran disponibles para el proyecto.

Los usuarios también deben participar y prestar apoyo a lo largo de la adquisición para asegurar que sus requisitos ha sido entendidos y que el resultado del sistema es aceptado y utilizado. La Participación de los usuarios debe mantenerse desde la fase de determinación de las necesidades del proyecto hasta la recepción definitiva y la ejecución del mismo.

La participación de los usuarios en el proceso de adquisición ayudará a evitar que no se cumpla con los requerimientos establecidos en el desarrollo y adquisición de los productos.

Los pasos de auditoría en esta sección pueden utilizarse para evaluar los riesgos potenciales que puedan surgir por la falta de gestión o soporte de usuarios. Una adquisición que carece de uno o ambos de estos elementos está en riesgo de incurrir en sobrecostos innecesarios, no cumplirá su calendario de entrega previsto y no logrará satisfacer las necesidades de la organización.

10.1.1 Objetivos de la auditoría

1. Asegurarse de que la alta gerencia brinde apoyo y participe activamente en todo el desarrollo y aplicación del proceso de adquisición.

2. Garantice que los usuarios participen activamente en el proceso de adquisición y en la definición de las necesidades, desarrollando el documento de solicitud de requerimientos y verificando que los equipos y / o servicios contratados satisfacen las necesidades de la organización.

10.1.2 Requerimientos Y Documentación

- Los Documentos, memorandos, u otros registros de la gerencia deben ser analizados y aprobados en los planes y objetivos de adquisición.
- La Gerencia de administración de programa u altos directivos que indicando objetivos y objetivos de la adquisición y la delegación de autoridad para llevar a cabo la adquisición.

- El Presupuesto y planos que indican la financiación del proyecto deben estar contemplados en el proceso de adquisición.
- Los planes del Proyecto que indican el papel de los usuarios en la planificación y en la supervisión de la adquisición. Toda la documentación de los roles de los usuarios en la validación de los requerimientos del proceso de adquisición, alternativas, y el pliego de condiciones. Roles de usuarios y responsabilidades pueden ser detallados en un memorando de entendimiento entre el usuario y la oficina del programa.
- Las Políticas de la organización o directrices sobre la estructura de comités de dirección o de otros órganos de supervisión, con responsabilidades de los miembros del proyecto y de la alta dirección.

10.1.3 Pasos de la Auditoría: Apoyo de la Alta Dirección

1. Identificar los funcionarios de alta dirección responsable del proceso de adquisición. Incluya funcionarios que están al frente de la administración de usuarios, funcionarios administradores de recursos de información y miembros de la alta dirección o comités directivos. Determinar los roles y responsabilidades de los grupo o comités de altos directivos y las relaciones entre ellos.

2. Revise la documentación relacionada con la adquisición y determinar si los altos directivos han identificado o tienen definido en el perfil de adquisición:

a. Aprobación de las metas y objetivos de la adquisición.

b. Designar a un patrocinador del programa que será el responsable en el proceso de la adquisición.

c. Establecer un proceso formal para mantener informada a las partes de cualquier cambio.

d. Participar en las revisiones específicas y decisiones.

- Determinar cómo las revisiones de la administración son realizadas y aprobadas y si las aprobaciones se dan en los niveles adecuados.
- Revisar la documentación de las revisiones, tales como memorandos de decisiones y minutas del comité de revisión.
- Determinar la frecuencia de las revisiones y la calidad de los administradores y personal que interviene en el proyecto.

e. Proveer fondos iniciales para el proyecto y establecer a corto y largo plazo los compromisos de financiación, periódicamente informar al comité de adquisición objetivos y situación del mismo.

f. Asegure todo el apoyo necesario de las principales organizaciones externas, como la OMB, GSA, y comités del Congreso.

g. Asignar funcionarios independientes para garantizar que la seguridad y los controles internos se cumplen.

3. Sobre la base de los pasos de la auditoría anterior y sobre contactos con administradores de otro proyecto, determinar si los altos directivos fomentan las buenas relaciones entre: el patrocinador, administrador de la adquisición (Director del programa), otros altos directivos, los técnicos de oficinas o jefes de departamento y la comunidad de contratistas. Específicamente, determinar si los administradores:

a. Coordinan acuerdos para el desarrollo de la evaluación, los planes de selección del recurso y lograr la aceptación del proceso de evaluación y los criterios.

b. Coordinan un acuerdo entre directivos del programa, el personal, técnicos y contratistas para la administración del contrato.

c. Obtienen el apoyo de los funcionarios encargados de la adquisición. Ya que es de vital importancia para la organización, como para el funcionario encargado de la selección del recurso.

4. Obtienen los usuarios y las evaluaciones del personal del proyecto que brinda apoyo a la gestión de los pasos anteriores. Averiguar el tiempo que tomó conseguir la aprobación de la administración y de dirección que dio al personal del proyecto.

10.1.4 Pasos de la Auditoría: participación de los usuarios

1. Identificar la población de usuarios de: Documentos del proyecto y los organigramas de la organización. Revise los criterios (reglamentos y procedimientos) para determinar las funciones o roles asignados a los usuarios.
Determinar el gestor del programa y seleccionar los usuarios que participan activamente en la adquisición. Identificar los grupos de usuarios importantes que no están involucrados en la adquisición.

2. Determinar si los usuarios:

a. Participan en las revisiones periódicas, y si es así, ¿cómo y con frecuencia están involucrados?

b. Darse de baja en las necesidades y las declaraciones de los requisitos o de lo contrario validar los requerimientos y soluciones correspondientes, cuando estén elaboradas.

c. Validar las alternativas frente a los requerimientos originales.

d. Aprobar la alternativa seleccionada (tales como las tecnologías disponibles en el mercado o desarrollo a medida, con procesamiento centralizado o distribuido, etc.)

e. Validar las especificaciones respecto a los requerimientos.

f. Proporcionar criterios de aceptación.

g. Ayudar en la preparación y el pliego de condiciones la adjudicación del contrato (por ejemplo, un grupo representativo de usuarios podrán ayudar en el desarrollo de los criterios de evaluación y participar en la evaluación de las alternativas del equipo de selección del recurso).

h. Participar en las actividades posteriores a la adjudicación que pueden incluir instalación, prueba y aceptación de los equipos.

i. Participar en las revisiones de los documentos entregables elaborados por el contratista, como el diseño de especificaciones, análisis de sistemas y usuario y manuales de entrenamiento.

j. Participar en grupos de trabajo de contratistas del gobierno.

k. Participar en auditorias posteriores a la adjudicación para evaluar el grado de éxito de la adquisición.

3. Determinar si los usuarios asignaron tiempo del personal y otros recursos para el proyecto.

4. Determinar si los usuarios participan en el programa tienen una tasa de rotación alta, moderada o baja.

5. Evaluar el apoyo financiero de los usuarios que soportan el proyecto.

a. Obtener el compromiso de financiación de los usuarios.

b. Identificar los créditos que deben ser usados y su disponibilidad para apoyar la adjudicación del contrato.

10.1.5 CobiT Recomienda…

- Entrevista con personal clave acerca de crear la conciencia en el grupo de usuarios y el conocimiento de los proceso para que el uso del sistema se haga de una manera eficaz y eficiente usando los sistemas de aplicación que soportan los procesos del negocio. (por ejemplo, la formación y desarrollo de capacidades, materiales de capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, soporte de mesa de servicio, la identificación del usuario clave, evaluación).

- Revisión de formación y materiales de aplicación para determinar si el proceso definido, incluye el contenido requerido.

- Confirmar a través de entrevistas con miembros clave que el usuario es consciente y capaz de utilizar el mecanismo de retroalimentación para evaluar la adecuación de la documentación de apoyo, procedimientos y capacitación relacionada.

11.2 PERSONAL IMPLICADO EN EL PROYECTO

La Administración de proyectos para una adquisición se lleva a cabo principalmente por un gerente de proyecto y un personal responsable de llevar a cabo las actividades del mismo.

El director del programa debe tener suficiente autoridad y una combinación adecuada de habilidades y experiencia para manejar con éxito el proyecto.

Al personal del proyecto de adquisición se le debe asignar muy claramente sus roles, funciones y responsabilidades. El equipo debe incluir miembros que son expertos en la información proceso de adquisición de tecnología, entender la tecnología y tener experiencia en la administración de contratos. El equipo también deberá tener miembros con conocimientos sobre los programas que la adquisición apoyará.

Objetivo de la Auditoría: Determinar si el equipo de adquisición tiene las habilidades necesarias y la autoridad para planificar eficazmente y ejecutar el proyecto.

11.2.1 Documentación Necesaria:

• Una lista de los principales miembros del equipo del proyecto mostrando sus responsabilidades, cargos, y la experiencia. El auditor puede generar esa lista sobre la base de las entrevistas si alguno de ellos no está disponible.
• La solicitud de contratación para que una delegación de facultades de adquisición de GSA, mostrar los nombres y experiencia de los funcionarios de proyecto

11.2.2 Pasos de Auditoría: administración del Proyecto

1. Revisión de los criterios de adquisición para determinar la responsabilidad y la del individuo que rendirá cuentas al director del proyecto y sus condiciones requeridas.

2. Revise la documentación relacionada con la adquisición para determinar la claridad de la responsabilidad del administrador del proyecto o en su defecto asignarla o definirla. Determine si el director del programa cuenta con:

a. Una carta para establecer la autoridad, responsabilidad y rendición de cuentas.

b. Una relación claramente definida con el proyecto, técnica, y las oficinas de contratación.

c. Una relación claramente definida con el patrocinador y usuarios.

d. Acceso a altos funcionarios de la Organización.

e. La autoridad para administrar los fondos de la adquisición.

f. La entrada al proceso presupuestario.

3. Revise las calificaciones de los responsables del Proyecto para determinar si el administrador del mismo tiene la combinación adecuada de habilidades y experiencia. ¿Ha realizado el director del proyecto otros proyectos de similar tamaño y complejidad? Es él o ella capacitados para manejar adquisiciones complejas.

4. revisión de la continuidad de la administración de la adquisición como lo demuestra el índice de rotación de los directores de proyectos.

11.2.3 Pasos de Auditoría: Personal del proyecto

1. Revisión de los criterios de adquisición del proyecto para determinar tanto la responsabilidad y la rendición de cuentas del personal de proyectos, así como su necesaria calificación.

2. Revisar la composición del equipo del proyecto para garantizar que la combinación de las habilidades del personal de la adquisición son adecuadas.

a. Determinar la autoridad y el nivel de experiencia de la Representante Técnico de contratos.

b. Identificar personal clave del proyecto y revisar sus experiencias y calificaciones. Determine si el funcionario contratante está entrenado y con experiencia en la adquisición de tecnología de la información.

c. Determine si el personal del proyecto tiene experiencia en la administración de los contratistas.

d. Determine la medida del volumen de negocio en el personal del proyecto.

3. Determine si el personal del proyecto se capacita para mantener sus competencias y calificaciones.

4. revisión de la razonabilidad de los hitos del proyecto y el calendario con los miembros del equipo del proyecto.

11.3 NECESIDADES / REQUERIMIENTOS / ESPECIFICACIONES

El propósito de este capítulo es orientar al auditor en determinar si la Alta Gerencia ha desarrollado una descripción precisa de su tecnología, información y necesidades. La adquisición debe estar claramente vinculadas al las necesidades del programa, a las estrategias generales de la Alta Gerencia, y el gobierno en cuanto a políticas y normas.

La Alta Gerencia debe ampliar su descripción básica de sus necesidades definir los requisitos específicos para que los proveedores de tecnología de la información puede responder con soluciones significativas. En algunos casos, una Alta Gerencia puede utilizar prototipos para ayudar a definir o validar sus necesidades. Los requisitos luego forman la base para aún más especificaciones detalladas.

En la identificación de sus necesidades, una Alta Gerencia debería realizar un plan para probar los recursos de información que necesita. Estos planes deben integrar la aceptación, la seguridad y requisitos de certificación. La prueba de los planes desarrollados en este punto forma la base para las evaluaciones posteriores de ejecución del contrato.

La falta de claridad y precisión en la definición de requisitos de tecnología informática presenta elevados riesgos para cualquier Alta Gerencia. Por ejemplo, una mala definición de requisitos puede reprimir las alternativas, restringir la competencia, aumentar el riesgo de costos y tiempos, y dar lugar a sistemas que son incompatibles con la arquitectura general de un organismo e incompatibles con los sistemas de otro sistema.

El hardware o software también puede ser inconsistente con las normas gubernamentales. Diseñar y aplicar un sistema es también más difícil si la entrada, la salida, y transformación de las especificaciones son incompletas o inexactas.

Además, si la seguridad y requisitos de control interno no están bien definidos, el control sobre la información sensible u otros bienes se perderá.

11.3.1 Objetivos de la Auditoria

1 Garantizar que la adquisición se basa claramente en las necesidades, oportunidades y que es coherente con la estrategia global y arquitecturas utilizadas por el organismo.

2. Asegurar que la Alta Gerencia define sus necesidades, basadas en las necesidades previamente identificadas y validadas por usuarios funcionales, lo suficiente como para apoyar la adquisición de hardware, software, telecomunicaciones, y sistema servicios de desarrollo. Estos requisitos deben ante todo ser expresados en términos funcionales de acuerdo con la política FIRMR.

3. Garantizar claridad en las especificaciones del sistema y precisión en el resumen de especificaciones de la Alta Gerencia.

11.3.2 Documentación Requerida

- Declaración de necesidades.
- Análisis de requerimientos o documento de requisitos funcionales

- Especificaciones del sistema, si se han preparado. También, proyecto de especificaciones con comentarios de la industria si las especificaciones del proyecto fueron liberados.
- Plan de pruebas y requisitos antes de la adjudicación del contrato. Requisitos de ensayo puede resumirse en una prueba y evaluación del plan maestro.

11.3.3 Pasos de la Auditoría: Determinación de Necesidades

1. Revisión de las necesidades expresadas de la Alta Gerencia, Que puede ser documentado en una declaración necesidades elemento misión, declaración de necesidad operativa, o concepto operativo del sistema. Determinar si las necesidades son claras y precisas y refleja las necesidades de los usuarios como se indica en la declaración de la misión y objetivos estratégicos de la organización de usuarios, la información del plan estratégico o plan de seguridad del ordenador.

2. Comprobar las necesidades de:

a. Existencia de arquitectura del sistema y las funciones de apoyo (es decir, descripción, costo, volumen de trabajo, proyecciones de crecimiento).

b. Justificación de los cambios, tales como la corrección, deficiencias en las capacidades existentes, cumpliendo con nuevos o modificados requisitos del programa, tomar ó aprovechar las oportunidades para mayor economía y eficiencia.

3. Póngase en contacto con varios usuarios, así como personal del proyecto que no son usuarios para determinar si están de acuerdo que el análisis de las necesidades presentadas en la declaración de necesidades. La suficiente atención a los problemas reales.

11.3.4 Pasos de Auditoria: Requerimientos Análisis

Revisar el análisis de los requisitos para determinar si describe el sistema actual. Esta descripción debe incluir todas las funciones del sistema actual que todo nuevo sistema tendrá que realizar. Los usuarios, funciones, carga de trabajo, gastos de explotación, y componentes del sistema actual también debe ser identificado.

2. Confirme que la Alta Gerencia ha definido su información requisitos para los recursos de información nueva.
Estos requisitos incluyen:

a. Información que actualmente se recibió o información que es necesaria, pero que no está siendo recibido.

b. Información que debe proporcionarse obtenidos de otros organismos o el público.

c. Fuentes disponibles de que para obtener la información necesaria.

d. Información de las relaciones.

e. El grado de validación de la información, la integridad, exactitud, integridad y confiabilidad.

f. La cantidad de información que se procesa y tipos de producción que se espera.

g. La puntualidad y el formato de la información.

h. La seguridad, la accesibilidad, y privacidad requisitos.

3. Determinar si la Alta Gerencia ha definido sus funciones y necesidades de apoyo, incluyendo:

a. Presente y cargas de trabajo proyectadas y la capacidad análisis, incluidos los requisitos de carga máxima y requisitos para la gestión de la capacidad futura.

b. Privacidad y seguridad.

c. Imprevistos necesidades de recursos cuya pérdida podría prevenir o intervenir para que la Alta Gerencia de cumplir con su misión o tendría un impacto negativo en la nación.

d. Documentos factores de manejo relacionados con la integración de los registros electrónicos con los registros de otros organismos, retención y disposición, y las salvaguardias contra el uso no autorizado o la destrucción de documentos.

e. El espacio y los factores del entorno, como el piso carga, la disipación de calor, y fuente de alimentación.

f. Las normas federales con el que la nueva tecnología deben cumplir.

g. necesidades de organización de formación.

h. Interfaces con otros sistemas.

i. Requisitos de usuario interfaz.

j. requisitos de compatibilidad de prescripción.

k. Capacidad o desempeño, requisitos de validación.

4. Determine si el análisis de requerimientos prevé lo siguiente:

a. Una metodología para que los usuarios validen los requisitos de análisis tanto para la capacidad y rendimiento.

b. requisitos mensurables que pueden ser utilizados más tarde para comprobar la eficacia del sistema.

5. Determinar si los requisitos se presentan en términos funcionales o de rendimiento en el examen de competencia total y abierta. Requisitos funcionales promover la competencia plena y abierta, mientras que requisitos rendimiento no pueden.

6. En cuanto a requisitos restrictivos (lo cual no condujeron a determinar la competencia total y abierta):

a. Si la marca de fábrica o igual o específica marca y modelo restricciones estén debidamente justificados.

b. Si todas las pruebas requeridas son completadas y aprobados para otra compatibilidad limitada requisitos.

7. Con respecto al proceso de revisión de requisitos durante la compra, determinar:

a. Ya sea un núcleo de necesidades básicas ha sido identificados a fin de mantener el alcance del proyecto.

b. Si un proceso de control de cambios formal ha sido establecido para administrar los cambios que se juzgue necesaria por un entorno cambiante.

c. ¿Quién es responsable de revisar y aprobar cambios en los requisitos?

d. ¿Con qué frecuencia los requisitos han sido cambiados?

e. Ya sea propuesto nuevos requisitos se validan con las necesidades de la misión.

f. ¿Qué proceso se utiliza para analizar los impactos de cambios en los elementos de las dos condiciones?

11.3.5 Pasos de Auditoria: Especificaciones

1. Determinar si los usuarios funcionales y / o el director del programa confirmó que las especificaciones reflejan con precisión los requisitos y se ajusten a la adquisición estrategia aprobada discutido en el módulo de adquisición de la estrategia. ¿Usuarios o el director de programa firmaron sobre las especificaciones de sistema?

2. Examine el documento de especificaciones:

a. Un resumen de los requisitos funcionales que se satisfecho por la tecnología.

b. Requisitos de funcionamiento evaluación.

c. Requisitos de funcionamiento que se ocupan de precisión de la información, requisitos de integridad de los datos; tiempo de respuesta, procesamiento de actualizaciones, la información transferencia, transmisión, y el rendimiento y la flexibilidad a los cambios en los requisitos.

d. Una identificación de nuevos tipos de equipos necesario (por ejemplo, procesadores, dispositivos de entrada / salida, o dispositivos de transmisión de información).

e. Una identificación de Soporte y software de prueba.

f. Una descripción de interfaces.

g. Una descripción general de seguridad y privacidad requisitos.

h. Una descripción de los controles operativos necesarios.

i. Una descripción de las características de funcionamiento del usuario y centros de computación en donde el software será utilizado.

j. Una descripción del flujo de la lógica de todo el sistema.

k. Una especificación de las funciones que deben cumplir el software.

3. Determinar cómo las restricciones a la libre y completo la competencia en el pliego de condiciones (por ejemplo, equipos características y elementos de calidad) son manipulados. Asegúrese de que todas las justificaciones requeridas están debidamente aprobadas para tales restricciones.

4. Determine cómo son manejados los cambios para las especificaciones originales

a. establecer la responsabilidad de examinar y aprobar los cambios a las especificaciones. Entrevista los usuarios a determinar si en realidad revisó y aprobó cambios en las especificaciones.

b. Revisar la documentación de las solicitudes de cambio.
Determine con qué frecuencia se cambian las especificaciones, si las nuevas especificaciones están validadas, y qué proceso se utiliza para identificar impactos de los cambios en otros elementos de pliego de condiciones.

5. Determine si el feedback (comentarios y preguntas) de los usuarios y la industria se explica, consideró, y se incorpora como sea posible sobre una base continua.

11.3.6 Pasos de Auditoria: Evaluación de Planes

1. Determinar si la Alta Gerencia ha desarrollado planes de prueba sobre la base de criterios de aceptación amuebladas o validadas por los usuarios.

2. Compruebe que ponen a prueba los planes de incorporar la seguridad y requisitos de certificación.

3. Determinar si la prueba los planes de medir adecuadamente el sistema requisitos de desempeño que se especificarán en la solicitud de propuestas (RFP).

11.3.7 CobiT Recomienda…

- Entrevista con miembros claves sobre la conciencia del personal de soporte técnico y operaciones y el conocimiento del proceso de manera eficaz y eficiente, soporte y mantenimiento del sistema de aplicación y la correspondiente infraestructura de acuerdo a los niveles de servicio (por ejemplo, la formación y desarrollo de capacidades, materiales de

capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, los escenarios de servicios de escritorio).

- Revisión formación y materiales de implementación para determinar si el proceso definido, incluye el contenido requerido.

- Confirmar a través de entrevistas con miembros clave del personal que el personal de soporte técnico y de operaciones es consciente y capaz de utilizar el mecanismo de retroalimentación para evaluar la adecuación de la documentación de apoyo, procedimientos y capacitación relacionada.

- Determinar si las operaciones y personal de apoyo están involucrados en el desarrollo y mantenimiento de las operaciones y la documentación de apoyo.

- Identificar las áreas donde los procedimientos de soporte operacionales no están integrados con los procedimientos de soporte operacional.

- Asegurar y confirmar que los cambios en las necesidades individuales son monitoreados, revisados y aprobados por los actores involucrados.

- Inspeccione la documentación pertinente para confirmar que todos los cambios y el estado de cambios se registran en el sistema de gestión del cambio.

- Identificar y comunicar los cambios a los que no se realiza un seguimiento.

11.4 ALTERNATIVAS

Después de identificar sus necesidades, la empresa debe evaluar las **alternativas** para examinar el costo-beneficio de dichos requisitos. La alternativa seleccionada, debe reflejar una comprensión de lo que está disponible tanto en el mercado comercial, como en el gobierno. Analizando cómo dicha alternativa apoya en el proceso de adquisición se reducen, pero no elimina, el riesgo de que otra compañía pueda seleccionar una alternativa que no satisfaga plenamente a los usuarios sus necesidades, u otras que sean innecesarias, complejas y de alto costo.

11.4.1 Objetivos de la Auditoría

1. Determinar si la Alta Gerencia ha considerado todos alternativas razonables para cubrir sus necesidades.

2. Determinar si la Alta Gerencia identifica los riesgos, los costos y beneficios de cada alternativa.

3. Comprobar que la Alta Gerencia seleccionada presente una alternativa equilibrada de los beneficios previstos con relación a los costos, tiempo y riesgos de fracaso.

11.4.2 Documentación Requerida

- Registro de análisis de alternativas, como un documento de decisión del sistema. Los análisis económicos y de riesgo deben acompañar o ser parte del documento de decisión.

- Encuesta con estudios de mercado llevada a cabo para identificar alternativas para las necesidades del usuario de reuniones y para apoyar las estimaciones de costos.

- Las conclusiones y declaraciones de apoyo a la aprobación de restricciones a las especificaciones, tales como limitación de los requisitos de compatibilidad.

- El costo / beneficio para justificar la selección de la alternativa seleccionada frente a otras alternativas, en términos de dólares o en términos de otros criterios, tales como la eficacia.

11.4.3 Pasos de Auditoría

1. Evaluar la participación de los responsables y verificar si:

a) Usuarios de acuerdo con el rango de alternativas consideradas y participaron en la validación de las alternativas con los requisitos originales.

b) Usuarios de acuerdo con la alternativa finalmente seleccionada.

c) Adecuada administración de quien aprobó la alternativa seleccionada.

d) El oficial de contrataciones u otro personal de contratación participaron en el análisis de alternativas para asegurar que un método de adquisición fue posible seleccionarlo.

e) El personal del proyecto que lleva a cabo estudios de mercado que determina cómo la industria puede cumplir mejor con los requisitos de la compañía.

2. Examinar cómo la Alta Gerencia realizó la evaluación de alternativas mediante la siguiente determinación:

a) El organismo constantemente analizan las alternativas con los mismos criterios para cada alternativa.

b) Las alternativas se describen con suficiente detalle para soportar el tiempo, estimaciones de costos y análisis coste / beneficio.

c) Las alternativas consideradas caben dentro de la arquitectura de información de la Alta Gerencia.

d) La gama de alternativas consideradas fueron restringidas por los presupuestos de recursos (las limitaciones de personal o de financiación).

3. Determinar si la Alta Gerencia constantemente realizan un análisis costo y beneficio de cada alternativa. Asegúrese de que el análisis económico incluye los valores actuales de costos y beneficios y que se actualicen periódicamente. Identificar la vida del sistema utilizado como base para evaluar las alternativas y determinar si parece realista o coherente a la luz de las necesidades del usuario, los cambios esperados en la tecnología, la disponibilidad esperada de mantenimiento y de soporte, y el tiempo necesario para preparar las adquisiciones posteriores.

Compruebe que el análisis económico incluye un análisis de sensibilidad para identificar los factores que afectan la elección de una alternativa sobre otra. Los costos y beneficios considerados para cada alternativa deben incluir:

a. Conversión de los costos.

b. Gastos de personal.

c. Costos de operación y mantenimiento.

d. No recurrentes, pero los beneficios cuantificables en términos de procesamiento de la información, administración y de soporte (éstos pueden incluir la reducción de costos resultantes de las operaciones del sistema mejorado o valor de la mejora a través de una mejor utilización de recursos).

e. Recurrentes y beneficios cuantificables en un mes y / o cada tres meses durante la vida útil del sistema de reducciones en artículos tales como salarios, beneficios sociales, suministros, servicios públicos y ocupación del espacio.

f. Los beneficios no cuantificables, tales como un mejor servicio e imagen de la organización.

4. Determinar si la Alta Gerencia analizó los factores de costo para cada alternativa posible:

a. Obsolescencia: estrategias para evitar los recursos obsoletos durante la vida útil del sistema. Una cláusula de actualización de la tecnología es una forma de evitar la obsolescencia, al permitir una Alta Gerencia para comprar versiones avanzadas de los equipos o software, cuando estén disponibles.

b. Disponibilidad: Hasta qué punto el sistema estará disponible para los usuarios.

c. Fiabilidad: La frecuencia con que el sistema requiere de mantenimiento correctivo.

d. Mantenimiento: la facilidad con que los componentes del sistema se puede reparar, para eso debemos tener en cuenta el nivel de servicio, personal de soporte, y los herramientas necesarias.

e. Optimización: la facilidad con que puede mejorar el sistema para satisfacer el requerimientos anticipadamente**.**

f. Flexibilidad: el grado en que la alternativa puede adaptarse a los cambios en la naturaleza de la carga de trabajo.

g. Seguridad: la capacidad de prevenir el acceso no autorizado y la manipulación y la consideración de la seguridad nacional y los preparativos de emergencia.

h. Privacidad: el grado de privacidad de los datos relacionados con el personal puede realizar mantenimientos.

i. Factores que afectan al personal: el impacto en el nivel del personal de soporte, incluyendo las habilidades requeridas.

j. Aceptación del usuario: el impacto generalmente en la comunidad de usuarios, incluyendo la cantidad de cambio a los procedimientos de usuario.

k. Rendición de cuentas: la capacidad de la alternativa de permitir la actividad del sistema para realizar el seguimiento y medida.

5. Revisar el análisis de riesgo para ver si identifica los datos sensibles y vulnerables. Compruebe la magnitud de cada vulnerabilidad identificada.

Determinar si el análisis de riesgo conforme a las normas señaladas en **FIPS** Publicaciones **65** y **73** y de la **OMB** Circular **A-130.**

6. Compruebe que cada alternativa se evalúa los riesgos financieros, técnicos y de programación. El riesgo financiero se refiere al grado en que cada alternativa está sujeta a costes adicionales inesperados. Riesgo técnico indica la probabilidad de que los objetivos técnicos de cada alternativa será difícil de lograr en su totalidad o en parte. Calendario de riesgo es el grado en que cada alternativa está sujeta a retrasos en el programa inesperado y el deslizamiento en el cumplimiento de los objetivos técnicos del sistema, sin importar el costo.

7. Asegúrese de que la Alta Gerencia ha seleccionado la alternativa más ventajosa y realista con respecto a los beneficios, costos y riesgos (basado en los pasos 4 y 7).

8. Compruebe que los usuarios y los altos directivos aprobar cualquier cambio en el alcance previsto del proyecto.

11.4.4. CobiT Recomienda…

• Confirmar a través de entrevistas con miembros o personales clave que en el proceso de adquisición y planificación de la estrategia de adquisición de TI estén alineados con las políticas de contratación de la organización y procedimientos (**por ejemplo**, requisitos legislativos, el cumplimiento de la organización de TI de la adquisición de la política, las licencias y los requisitos de arrendamiento, las cláusulas de actualización tecnológica, participación de la empresa, costo total de propiedad, el plan de adquisición de grandes adquisiciones y por último el registro de los activos).

• Revise las políticas de gestión y procedimientos de los proyectos para evaluar la conformidad con las políticas de contratación y los procedimientos de la empresa.

• Confirmar a través de entrevistas con miembros clave del personal que las políticas y normas dan lugar para el establecimiento de contratos con los proveedores. Las políticas y normas que debe abordar, las responsabilidades del cliente-proveedor, proveedor **SLA**, control e información contra la **SLA**, disposiciones transitorias, los procedimientos de notificación y la progresividad, las normas de seguridad, los requisitos de gestión de registros y control, y requiere prácticas de los proveedores de control de calidad. Los contratos deben incluir también una parte jurídica, financiera, documental de organización, funcionamiento, seguridad, auditabilidad, la propiedad intelectual, la responsabilidad y los aspectos de sus asistencias

• Confirmar a través de entrevistas con el personal clave con criterios predefinidos, específicos y establecidos (**por ejemplo**, la definición de los requisitos, calendario, proceso de decisión) se utilizan para la selección de proveedores y adquisición.

• Inspeccione las solicitudes de información (**RFI**) y solicitudes de propuesta (**RFP**) para determinar si los criterios establecidos se definen.

• Confirmar que las adquisiciones de software incluyen y hacen cumplir los derechos y obligaciones de todas las partes (**por ejemplo**, la propiedad y concesión de licencias de propiedad intelectual; garantías de mantenimiento, los procedimientos de monitoreo; términos de actualización y adecuación, incluida la seguridad, custodia y derechos de acceso). Para una selección de software adquisiciones, inspeccionar los documentos pertinentes y determinar si las condiciones del contrato incluyen los derechos y obligaciones de todas las partes.

• Determinar si el asesoramiento jurídico que se haya obtenido en los acuerdos de adquisición de recursos de desarrollo respecto a la propiedad y concesión de licencias de propiedad intelectual.

• Para una selección de las adquisiciones del desarrollo de los recursos, revisar la documentación pertinente y determinar si las condiciones del contrato incluyen los derechos y obligaciones de todas las partes.

• Confirmar que las adquisiciones de la infraestructura, instalaciones y servicios relacionados incluyendo el hacer cumplir los derechos y obligaciones de todas las partes (**por ejemplo**, el servicio los niveles, los procedimientos de mantenimiento, controles de acceso, seguridad, evaluación de desempeño, base para el pago, los procedimientos de mantenimiento).

• Para una selección de la adquisición de la infraestructura, instalaciones y servicios relacionados, inspeccionar los documentos pertinentes y determinar si las condiciones del contrato incluyen los derechos y obligaciones de todas las partes.

• Averiguar si y confirmar que las **IFR** y solicitudes de propuesta se evalúan de acuerdo con el proceso y criterios establecidos.

• Determinar si la evidencia documental es efectivamente mantenida.

• Determinar si todos los acuerdos de adquisición se verifican.

• Revisión de los acuerdos, se compara con la documentación de políticas y determinar si cumplen con la política de empresa.

• Determinar si las adquisiciones son revisados y aprobados por el personal apropiado y si el asesoramiento jurídico que se haya obtenido.

• Revise la documentación de la revisión y aprobación de contratos.

• Averiguar si los procesos comunes son establecidos y utilizados para la adquisición de software, la infraestructura y las instalaciones.

• Realizar un rastreo a través de los procesos para determinar si funcionan con eficacia.

• Averiguar si los derechos y obligaciones de todas las partes a la adquisición son evaluados en los procesos de adquisición. Estos derechos y obligaciones pueden incluir:

- Aprobación
- Niveles de servicio
- Los procedimientos de mantenimiento
- Controles de acceso
- Seguridad
- Evaluación del funcionamiento
- Base para el pago
- Arbitraje de los procedimientos

• Para obtener una muestra representativa de las adquisiciones, determinar si los derechos y obligaciones de todas las partes que se evalúan.

• Averiguar si el proceso de adquisición debidamente en cuenta todos los derechos y obligaciones pertinentes, que pueden incluir:

- La propiedad y concesión de licencias de propiedad intelectual
- Mantenimiento
- Las garantías y los procedimientos de arbitraje
- Actualizar los términos
- Aptitud para el uso, incluida la seguridad
- Depósito de garantía y los derechos de acceso

• Determinar si los requisitos de gestión de información asociados con las adquisiciones se abordan.

• Averiguar si una evaluación de la calidad y la aceptación de proceso para todas las adquisiciones ha sido creado y utilizado, y determinar si este proceso es eficaz a cabo en todas las adquisiciones antes del pago se hace.

• Averiguar si todas las adquisiciones de hardware y software se registran.

• Seleccione una muestra representativa de las adquisiciones y verificar que se registran en los registros de activos.

11.4.5. ISO 9000 Recomienda…

- Que dentro de las opciones de solución que ofrece la **ISO 9000** con respecto a los problemas que generalmente influyen la mala gestión de Calidad está la **revisión** de la política de calidad documentada orientándola hacia la calidad, los clientes, **proveedores** y mejoramiento continuo, realizando su ajuste. Así mismo partiendo de esta política de calidad que existía se subdividió para identificar de acuerdo a los objetivos de calidad, con los cuales debían trabajar todos los procesos de la entidad y sus colaboradores.

- Dentro de los principios de calidad, son el pilar de un S.G.C. cualquiera que sea su clase, una empresa que implemente estos principios está cumpliendo con cualquier norma certificable, dentro de los 8 principios que existen, nos interesa el No. 8 que es: **"Relaciones Mutuamente Beneficiosas con el Proveedor"**, este principio nos dice:

"Una organización y sus proveedores son interdependientes, una relación de beneficio mutuo refuerza la habilidad de ambos para crear valor.
Aplicar el principio *Relaciones mutuamente benéficas con proveedores* conduce a las siguientes acciones:

• Identificación y selección de proveedores clave.

• Establecer relaciones con proveedores que equilibren las ganancias del corto plazo, con consideraciones de largo plazo, para la organización y la sociedad en su conjunto.

• Crear comunicaciones claras y abiertas.

• Iniciar de manera conjunta el desarrollo y mejora de productos y procesos.

• Establecer en conjunto un entendimiento claro de las necesidades del cliente.

• Compartir información y planes futuros.

• Reconocer las mejoras y logros del proveedor.

Aplicaciones benéficas de este principio incluyen:

• ***Para el desarrollo de las políticas y estrategias,*** la creación de las ventajas competitivas mediante el desarrollo de alianzas estratégicas o asociaciones con los proveedores.

• ***Para fijar objetivos y metas,*** establecer objetivos y metas más retadores mediante el involucramiento y participación temprana de los proveedores.

• Flexibilidad y rapidez de respuesta de forma conjunta a un mercado cambiante o a las necesidades y expectativas del cliente.

• ***Para la gestión operativa,*** crear y administrar relaciones con los proveedores para asegurar el suministro de bienes de manera confiable, a tiempo y sin efectos.

• Optimización de costos y recursos.

• ***Para la gestión de los recursos humanos,*** desarrollar e incrementar las capacidades de los proveedores, a través del entrenamiento y esfuerzos conjuntos de mejora.

• Aumento de la capacidad de crear valor para ambas partes.

Al estar integrados con la organización, los proveedores, han de adaptarse rápidamente a las necesidades de la empresa si quiere mantener su nivel de negocio o aumentarlo. Si el proveedor, no es capaz de satisfacer las necesidades de la empresa, no se podrán satisfacer las necesidades de los consumidores**2.**

- Por último en la sesión **7.4** de los requerimientos que exige esta norma **ISO de calidad** es la llamada: **"Compras"**.

2 INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de calidad. Fundamentos y vocabulario. Santa Fe de Bogotá: 2000. (NTC ISO 9000) Págs. Vi-Vii.

Esta sesión menciona **3 incisos** que hablan del proceso de **compras** como tal, la información requerida y para realizar un buen trabajo de compras, se menciona los aspectos de la verificación de lo comprado. A continuación se citan los 3 puntos que son muy importantes a la hora de una adquisición de un producto y/o servicio (en este caso de estudio, **Adquisición de software**).

Proceso de compras

La organización debe asegurarse de que el producto adquirido cumple los requisitos de compra especificados. El tipo y el grado del control aplicado al proveedor y al producto adquirido deben depender del impacto del producto adquirido en la posterior realización del producto o sobre el producto final.

La organización debe evaluar y seleccionar los proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización. Deben establecerse los criterios para la selección, la evaluación y la re-evaluación. Deben mantenerse los registros de los resultados de las evaluaciones y de cualquier acción necesaria que se derive de las mismas

Información de las compras

La información de las compras debe describir el producto a comprar, incluyendo, cuando sea apropiado:

a) Los requisitos para la aprobación del producto, procedimientos, procesos y equipos,
b) Los requisitos para la calificación del personal, y
c) Los requisitos del sistema de gestión de la calidad.

La organización debe asegurarse de la adecuación de los requisitos de compra especificados antes de comunicárselos al proveedor.

Verificación de los productos comprados

- La organización debe establecer e implementar la inspección u otras actividades necesarias para asegurarse de que el producto comprado cumple los requisitos de compra especificados.

- Cuando la organización o su cliente quieran llevar a cabo la verificación en las instalaciones del proveedor, la organización debe establecer en la información de compra las disposiciones para la verificación pretendida y el método para la liberación del producto**."**[3]

3 INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de calidad. Fundamentos y vocabulario. Santa Fe de Bogotá: 2000. (NTC ISO 9000) Capítulo 7.4

11.5 PLAN DE ADQUISICIÓN

La planificación de la adquisición es el proceso de coordinar e integrar los esfuerzos del personal responsable de las adquisiciones. Uno de los objetivos principales de la planificación de la adquisición, es el de promover y garantizar una competencia plena y abierta.

Para asegurar que la planificación se lleva a cabo de manera eficaz, económica y oportuna, la Alta Gerencia deberá preparar un plan de adquisición que contenga una estrategia global para la gestión de la aprobación previa, la adquisición, y las fases posteriores de adjudicación.

Un plan de adquisición efectivo, es crítico para el éxito del proyecto. El plan establece lo que la Alta Gerencia va a hacer para completar una compra y cómo lo hará. El plan también especifica el tipo de contrato que será adjudicado, cómo la Alta Gerencia seleccionará un contratista, costo y el cronograma de metas, hitos, áreas importantes de riesgo y los controles de gestión de contratos.

Los auditores deben evaluar el grado en que la planificación de adquisición de la Alta Gerencia es realista y completa. Una parte de esta evaluación debe ser la revisión de la solicitud de la Alta Gerencia Pública (APR) para determinar si están completos y reflejos con precisión los objetivos y el alcance del proyecto.

11.5.1 Objetivo de Auditoría

Comprobar que la Alta Gerencia ha definido una estrategia efectiva y un plan para la selección de un contratista y la gestión de la ejecución del contrato.

11.5.2 Documentación Requerida

- Plan de Adquisición y los documentos relacionados a su caso, como un plan de acción y metas.

- Solicitud de la Alta Gerencia de adquisición y otro tipo de correspondencia con la GSA.

11.5.3 Pasos de Auditoría

1. Determine si el plan de adquisición fue revisado y aprobado de manera oportuna por los funcionarios designados bajo las normas de adquisición de la Alta Gerencia. Asegúrese de que el director del programa revise periódicamente el plan de adquisición y actualizaciones cuando sea necesario.

2. Revise el plan de adquisición y determine si contiene los elementos requeridos por el **FAR** en la Sección 7.1 y la información de Tecnología de **GAO**: Un modelo de ayuda para administrar la Disminución de riesgos de adquisición.

Estos elementos incluyen los objetivos de la adquisición y de coste; responsables encargados de la toma de decisiones; características de capacidad o de rendimiento; los riesgos asociados con cuestiones técnicas, de programación y costos; plan de acción; los procedimientos de selección de fuente; la competencia de tipo contractual y las disposiciones especiales del contrato; procedimientos de gestión o de organización, presupuesto y financiación; la información necesaria para supervisar el desempeño de los contratistas, de pruebas y evaluación de seguridad y privacidad; y los hitos de adquisición.

El plan también debe identificar el método de adquisición, la llave "go / no-go, un plan de capacitación formal, y un plan de contingencia para minimizar las pérdidas.

3. Determine si el plan de adquisición realiza una llamada para una competencia total y abierta. Si las llamadas al plan de adquisición son limitación de los recursos compatibles con el equipo existente, compruebe que la conversión de los estudios de costos ha llevado a cabo para justificar las restricciones de compatibilidad. Si el plan de llamadas para distintos a la competencia plena y abierta, compruebe que las restricciones a la competencia, como marca y modelo de las restricciones o requisitos de fuente única, se han justificado y aprobado por la autoridad designada.

4. Determinar si la Alta Gerencia tiene planeado un "**gran diseño**" del proyecto o la adquisición organizada por módulos. La compra incremental puede minimizar los riesgos mediante la identificación de los eventos pasados, lo que permite una mayor facilidad en la corrección.

5. Evaluar las herramientas de gestión de proyectos y técnicas para satisfacer los requisitos de gestión de la información para monitorear el desempeño del contratista, el seguimiento del progreso contra el plan de adquisición y la adopción de medidas en el deslizamiento de costes o el cronograma.

6. Revisión del programa de la Alta Gerencia para el desarrollo del pliego de condiciones y para las actividades de selección base. Evaluar la razonabilidad de la programación a través de discusiones con los funcionarios de contratación ya los exámenes de progreso del proyecto.

11.5.4 CobiT Recomienda

• Confirme con el personal el plan para la adquisición, aplicación y/o actualización de la infraestructura de tecnología se ha creado el negocio que satisfaga requisitos funcionales y técnicos.

• Revisar el plan para confirmar que cumpla con la dirección tecnológica de la organización establecida y que todos los aspectos clave se incluyen.

• Averiguar si y confirmar que un proceso se ha definido e implementado para crear y mantener un plan de adquisición de infraestructura que está alineado con el organización de la dirección tecnológica.

• Inspeccione el plan de adquisición de infraestructura para identificar las áreas en aspectos clave, tales como los requisitos, los riesgos, la transición y la migración, no se han abordado.

• Revisión de la evaluación financiera para la exactitud y la cobertura global

11.6 DOCUMENTO DE LICITACIÓN

11.6.1 Documento de Licitación

Un documento de licitación proporciona información necesaria a los vendedores para proponer equipos, software y servicios para satisfacer los requisitos o requerimientos de la organización. En la mayoría de los casos, los recursos de información se adquirirán mediante la emisión de una solicitud de propuesta, que constituye la base para el contrato resultante. Con menos frecuencia, una organización podrá adquirir los recursos de información mediante una invitación a

presentar ofertas. Una solicitud de propuesta puede ser precedida por una solicitud de información o solicitud de cotización.

Una solicitud de propuesta debe ser clara y completa, incluirá los elementos descritos en las directrices de la GSA en el documento estándar de licitación.

En el desarrollo de la RFP, una organización puede tener pre solicitación o propuesta preliminar con el fin de recabar las opiniones de la industria sobre el proyecto de adquisición y alentar a las empresas para ofrecer propuestas. Una vez que el RFP se desarrolla, puede ser liberado en forma de proyecto para obtener las preguntas y reacciones de la industria.

Los auditores deben determinar que medidas la organización debe adoptar para conseguir información sobre sus requerimientos, como la organización ha manejado los comentarios o preguntas en una propuesta RFP, y si la organización ha tomado medidas para garantizar que las propuestas del contratista son competitivas.

Un buen RFP es un elemento crítico del éxito de la adquisición, ya que se convierte en parte de la unión del contrato una vez que se hace una propuesta y es aceptada. Si el RFP no es exacto y describe claramente los requisitos de la organización o si los factores de evaluación no se reflejan con precisión en las prioridades de la organización, entonces el resultado de la adquisición no va a satisfacer las necesidades del usuario. Si la Solicitud de la Propuestas es injustificadamente restrictiva, lo que favoreciendo a uno de los contratistas sobre los demás, el organismo puede ser incapaz de beneficiarse de la competencia total y abierta.

Los auditores deben familiarizarse con el formato estándar de la RFP para una solicitud de propuesta. El equipo de auditoría debe incluir personas que sean

suficientemente conocedoras de la tecnología de la información que debe ser adquirida para juzgar así que la organización ha definido sus necesidades en la Solicitud de la Propuesta.

Los miembros del equipo debe incluir o tener acceso a personas que pueden identificar áreas en las que el RFP no haya defino en los requerimientos de la organización lo suficientemente bien como para proteger el gobierno de sus intereses.

Estas personas también deben saber lo suficiente sobre el rendimiento o la técnicas de validación de capacidad para determinar si o no los requisitos de la organización son razonables y eficaces.

11.6.2 Objetivo de la Auditoria

Determinar si el documento de licitación esta completo, clara y coherente. Compruebe que los requerimientos siguen reflejando las necesidades del usuario, y determine si el proceso de evaluación propuesto da lugar a una adquisición eficaz y económica.

11.6.3 Documentación Requerida

• Registro de la pre solicitud o propuesta preliminar.
• Documento de Solicitud: solicitud de propuesta o invitación para la oferta.
• Informe de un comité de revisión de solicitud o de una comisión, si es apropiado.
• Plan de selección del recurso.
• Materiales de referencia o de otras capacidades y requerimientos de validación de rendimiento.

• Comentarios del proveedor o preguntas sobre el documento de solicitud.
• Guía de evaluación Propuesta.

11.6.4 Pasos de Auditoria:

1. Determinar si el pliego de condiciones contiene:

a. la declaración de trabajo o especificaciones de la declaración que con claridad y precisión describen los requerimientos de la organización, incluyendo una clara definición de todos los materiales y las condiciones de su aceptabilidad.

b. Una definición clara de las responsabilidades del gobierno y el contratista.

c. La importancia relativa de los factores de evaluación.

d. Un formato de propuesta que requiere que el costo y los elementos técnicos estén separan.

e. Provisiones razonables que protejan la organización (Tales como daños y perjuicios) o dar incentivos al contratista (por ejemplo, bonos de buen desempeño).

2. Examinar los criterios de evaluación para asegurar:

a. Son consistentes con el análisis de los requerimientos, especificaciones y las instrucciones de la preparación de la propuesta.

b. Proporcionan todos los factores e sub factores significativos que considerar en la evaluación de ofertas y la importancia relativa de las diferentes técnicas o los factores de costo, de acuerdo con FAR 15.605.

3. Evaluar el desempeño del paquete de evaluación de la empresa que se usará. Determinar si la organización reembolsa a los contratistas para participar en evaluaciones y otras pruebas, y si el costo de esas actividades de evaluación del desempeño constituye un obstáculo para la competencia.

a. Si hay un punto de referencia, ¿está siendo independientemente examinado por alguien fuera de la organización? Revise el plan de referencia para confirmar que los criterios de demostración son claramente declarados. Determinar cómo la organización seleccionó una mezcla representativa de los programas de referencia.

Determinar si la complejidad de los programas en el punto de referencia es representativa. Determinar cómo la organización validó el punto de referencia como representativo.

b. Si hay simulación o modelado, determinar cómo la organización selecciono los parámetros para el modelo. Revisar todas las inquietudes o quejas planteadas por los proveedores.

4. Entrevista con los usuarios y administradores, en caso necesario, para determinar si están de acuerdo con la solicitud. Determinar si los usuarios o los administradores han identificado nuevos requerimientos no incluidos en el RFP. Identificar criterios de evaluación u otros factores incluidos injustamente para restringir la competencia.

5. Revisar el plan de selección de recurso de la organización para asegurar que describe claramente la selección del recurso y actividades. Asegúrese de que el plan de selección del recurso ha sido aprobado por la administración antes de que el pre solicitación se lleve a cabo o el documento de solicitación es emitido, en acuerdo con FAR 15.612.

6. Revisión del proceso de retroalimentación y determinar si:

a. Los Comentarios recibidos sobre el proyecto de solicitud necesitan aclaración, restrictivas especificaciones, o formas alternativas de satisfacción de las necesidades de los usuarios.

b. La organización respondió rápidamente a los comentarios recibidos.

c. La información brindada es adecuado sobre la disponibilidad del producto en el mercado.

d. El uso de un mediador facilita el proceso de abordar las preocupaciones de los proveedores, las disputas, y quejas.

7. Determinar quién ha realizado revisiones legales en el documento de la solicitud.

8. Determine si cualquier proveedor ha presentado una protesta, cuándo y cómo se resolvió. Determinar la base de la protesta y su resolución.

11.7 SELECCIÓN DE RECURSOS

El proceso de selección del recurso es crítico para asegurar el mejor valor para el gobierno. Todas las propuestas deben ser evaluadas de acuerdo a los criterios publicados en el RFP. Si el proceso de evaluación no se ajusta a la solicitud de ofertas de la Alta Gerencia, corre un riesgo mayor de que la respuesta de la oferta conlleve a la pérdida de los vendedores.

La Alta Gerencia debe recibir las propuestas, evaluar la parte técnica y los méritos de las diferentes propuestas, negociar con los contratistas y adjudicar un contrato con arreglo a un plan de selección de fuente desarrollado antes de la liberación de la RFP.

El auditor debe ser consciente de la organización y procedimientos que la Alta Gerencia para la adopción de un contrato. Las Alta Gerencias pueden usar algunas o todas de las siguientes posiciones:

- Oficial de Contratación (CO). El Oficial Contratante publica el documento de contratación, adicionalmente, modifica el RFP si es necesario, y lleva a cabo todas las negociaciones con oferentes.

- Fuente de selección de Autoridad (SSA). La SSA efectúa la decisión final sobre la adjudicación del contrato. El Órgano de Contratación Responsable podrá ser la SSA para algunas compras, mientras que en otros casos un director de mayor rango puede servir como SSA.

- Fuente del Consejo Asesor de Selección (SNCC). El SSAC aporta opiniones de las evaluaciones de las diferentes propuestas y hace una recomendación a la SSA en el contrato premio.

- Selección La Junta de Evaluación (SSEB). El SSEB lleva a cabo evaluaciones técnicas y de costos de las propuestas del proveedor.

11.7.1 Objetivos de la Auditoría

Garantizar que el proceso de selección de la fuente sea planificado y llevado a cabo para alcanzar con éxito un contrato que dé el mejor valor para el gobierno.

11.7.2 Documentación Requerida

- La selección de plan, incluyendo la selección de la organización base.
- Informe de las lecciones aprendidas u otro informe por el Funcionario contratante que describe las negociaciones y las actividades de selección.
- Archivo de contratación del Oficial de contrato.
- Los registros de reuniones informativas, si es pertinente.
- Resultados de los puntos de referencia o el rendimiento y otras técnicas de validación de la capacidad utilizada.
- La correspondencia entre los oferentes y la Alta Gerencia respecto a las preguntas o aclaraciones y cualquier enmienda a la RFP.
- Propuesta de guía de evaluación.
- Revisiones pre auditoría.

11.7.3 Pasos de Auditoría

1. Examinar el proceso de evaluación mediante la revisión de registros de los procedimientos de selección de fuente y determinar:

- **a)** Aplicar el proceso de evaluación y criterios de publicidad en la solicitud al personal de evaluación de una manera Estricta.
- **b)** Que los factores de evaluación que se aplicaron estén o no enumerados en la solicitud.
- **c)** Ya sea que los costos y las evaluaciones técnicas se realizaron por separado.
- **d)** El papel que juegan los usuarios en el proceso de evaluación.
- **e)** Si el proceso ha resultado en (1) el establecimiento de una lista de competidores y (2) eliminación de los oferentes de un nuevo examen, de conformidad con el FAR 15,609.

2. Determinar cómo los proveedores recibieron la solicitud y la cantidad de propuestas presentadas.

3. Determinar si el organismo de fijación de precios obtenidos de campo apoyo, de conformidad con el FAR 15.805-5. ¿Fue una auditoría previa de adjudicación de la propuesta de costes logrados y utilizados durante las negociaciones? ¿Si el oferente de tarifas propuestas en comparación con los directos, indirectos, gastos generales, y las tasas generales y administrativos recomendadas por la auditoría contrato correspondiente la actividad?

4. Examinar el proceso de negociación.

- **a)** Confirme que las discusiones con todos los vendedores en el gama competitiva y se llevaron a cabo los trabajos de la documentación.

b) Determinar a partir de una revisión de la documentación de los controles existentes para proteger la seguridad de información confidencial.

c) Póngase en contacto con los funcionarios responsables de sus evaluaciones de la seguridad.

d) Determinar si los costos estimados del ciclo de vida se conciliarse con la propuesta de cada proveedor para garantizar que las estimaciones de costes parecen realistas.

5. Examinar cómo el organismo maneja mejor y final ofertas.

a) Determinar si la Alta Gerencia hizo varias llamadas para ofrece lo mejor y final, justificada con arreglo al FAR 15.611.

b) Determine si ofrece lo mejor y final fueron solicitados a evaluar de acuerdo con la fuente plan de selección.

6. Determinar si todos los informes finales:

a) Fueron programados tan pronto como sea posible cuando sean solicitado por el vendedor.

b) Se basan en un plan de interrogatorio para abordar problemas no resueltos que puedan causar preocupación y quejas entre los vendedores perder.

c) Se documentaron

7. Examine el esfuerzo realizado para identificar las lecciones aprendidas.

a) Determinar cuáles son las políticas o los procedimientos del organismo los usuarios tienen que evaluar los resultados de la adquisición y comunicar las "lecciones aprendidas" para el personal que efectúe futuras asignaciones y otros organismos. ¿Estos incluir una comparación de la concesión previa de las actividades del plan de adquisición?

b) Revise el informe de lecciones aprendidas, si uno se terminado, para determinar cómo los funcionarios del organismo evaluar el proceso de contratación.

11.8 GESTIÓN DE CONTRATOS

El contrato incluye la gestión de los pasos necesarios para asegurarse de que la Alta Gerencia recibe productos y servicios dentro de los costos y los plazos establecidos. Una Alta Gerencia tiene la obligación de vigilar el desempeño del contratista, garantizar que el trabajo realizado se ajusta a los requisitos de la Alta Gerencia. La misma, también debe controlar los cambios del contrato y aceptar o rechazar los resultados finales. Por último, una Alta Gerencia debe llevar a cabo Reseñas de post implementación para determinar qué tan bien objetivos de adquisición se cumplen y si los recursos de información adquiridos deben ser añadidos o sustituidos.

La Alta Gerencia oficial de contrataciones y Contratación Representante oficial de / Oficial de Contratos Representante Técnico tienen la responsabilidad primaria de la administración del contrato. El Órgano de Contratación Oficial de monitores como los costos requeridos por el tipo de contrato (a precio fijo o reembolso de los gastos) y hace modificaciones del contrato, según sea necesario.

El programa administrador de ayuda a monitorear el desempeño del contratista a garantizar que se cumplen los requisitos del usuario por los productos o servicios prestados y la tercera edad que funcionarios de proporcionar apoyo y supervisión.

El contrato consiste en RFP de la Alta Gerencia, en su versión modificada, y la propuesta del vendedor exitoso. El contrato debe especificar todos los aportes necesarios del proveedor. El Oficial de Contratos y Contratación Representante oficial de / Oficial de Contratos Representante Técnico debe asegurarse de que prestaciones que se reciban como sea necesario. Cualquier situación e informes de costos requeridos por el contratista deben revisión y las medidas adoptadas para corregir los problemas, si es necesario. Formación, documentación y mantenimiento requisitos se deben cumplir.

11.8.1 Objetivos de Auditoria

Para asegurarse de que la Alta Gerencia:

1. Supervisa el desempeño del contratista.
2. Asegura que los requisitos del contrato continuará
reflejan con precisión las necesidades de los usuarios.
3. Verifica que los productos y servicios entregados cumplen
necesidades de los usuarios.
4. Realiza una gestión de configuración.
5. Modifica el contrato sólo cuando sea necesario.
6. Aplica las disposiciones del contrato destinado a proteger
la Alta Gerencia, tales como garantías o daños y perjuicios
cláusulas.

11.8.2 Documentación requerida

- ✓ Alta Gerencia de reglamentos o directivas especificando requisitos para las revisiones periódicas, la gestión supervisión y administración de configuración.
- ✓ El contrato adjudicado y con las modificaciones.
- ✓ La organización de la Alta Gerencia de gestión de contratos y estructura.
- ✓ informes sobre la situación actual y el costo o el horario proyecciones.
- ✓ informes sobre el presupuesto actual.
- ✓ El plan de gestión de configuración para el proyecto.

11.8.3 Pasos de Auditoria

1. directivas de revisión de la Alta Gerencia para identificar la Alta Gerencia requisitos para la supervisión del contrato. Departamento de Defensa estándar 2167A, por ejemplo, requiere exámenes periódicos de las prestaciones del contrato, con un coste e informes de estado por parte del contratista. Defensa también ha directivas que rigen la gestión de configuración actividades para asegurar que el contratista entrega el equipos o servicios solicitados y que no hay cambios en el contrato se hizo sin tener en cuenta su impacto global.

2. Identificar los roles de los usuarios y administradores de alto nivel en seguimiento del contrato, verificando que los usuarios y los altos directivos están implicados en la gestión del contrato y la aprobación de cualquier cambio.

3. Determinar el nivel de autoridad y la experiencia de la Oficial de Contratos Representante o Contratante Representante Técnico Oficial.

4. Evaluar el personal del proyecto.

a. Identificar al personal clave del proyecto y revisar su experiencia y calificaciones. ¿Es el Órgano de Contratación Oficial de formación y experiencia en la información adquisición de tecnología? ¿Incluye el proyecto personal con experiencia en la gestión de los contratistas?

b. Determinar la cantidad de volumen de negocios no ha sido en el personal del proyecto, incluyendo el proyecto gerente.

5. Evaluar los cambios a los requisitos de la Alta Gerencia de garantizar que el contrato sigue reflejando válida necesidades de los usuarios. Examen de la gestión de configuración actividades para verificar que los cambios en los requisitos son impactos registrados y controlados y que los cambios a los requisitos del contrato están identificados.

6. Evaluar los cambios en los costos de la Alta Gerencia y el calendario estimaciones. ¿Si las variaciones en el costo y el horario proyecciones seguido por el director del proyecto o Contratante Representante Técnico de? ¿Si estimaciones de costos y el calendario modificado apropiadamente?

7. Determinar si la Alta Gerencia de supervisión de los contratistas rendimiento incluye:

a. La revisión periódica de los regulares y completado los aportes y eficaz reacción los retrasos. Determinar cómo la Alta Gerencia se compara contratista de progreso con el contrato de trabajo horario.

b. La revisión periódica de informes contrato. Revisar una muestra de informes de situación y el costo para comprobar que regularmente presentado por el contratista como exigir el contrato. Discutir su utilidad con el personal del proyecto.

c. La evaluación de la adecuación de la calidad del contratista garantía de proceso.

8. Evaluar la efectividad de los trabajo de la Alta Gerencia relación con el contratista.

a. Verificar que la Alta Gerencia ha controlado los cambios en el contrato e integrada del proceso de cambio en el adquisición de la estructura de gestión. Determinar el impacto de los cambios en el costo del contrato y el calendario.

b. Determinar si las correcciones se hacen, los premios son implementado, y daños y perjuicios, como apropiado.

9. Determinar si el contrato de Alta Gerencia de los controles modificaciones por:

a. Exigir la oficina de contrataciones de aprobar toda la modificación de los contratos.

b) El establecimiento de un proceso de revisión para garantizar que cambios propuestos de ingeniería están dentro del alcance del contrato.

c) Regularmente comparar los gastos del contrato con la delegación de facultades de adquisición para asegurar que la Alta Gerencia no sea superior a su nivel autorizado de los gastos totales

11.9 PRUEBA Y ACEPTACIÓN

Las pruebas proporcionan la base para la toma de decisiones en cuanto a conveniencia de contratos se refiere. Para la obtener eficacia en la realización de pruebas estas deben ser dirigidas relativamente al proceso de adquisición para que este pueda ser adecuadamente comprendido en la planificación. Los planes de pruebas proporcionan evidencias de los procedimientos y los criterios de evaluación para evaluar los resultados.

La alta gerencia debe establecer sus planes de prueba inicial en la fase de pre solicitación. Estos planes deben mostrar cómo el organismo verificará que el equipo adquirido, software o servicios cumplen con las necesidades del usuario y satisfacen los requisitos de seguridad.

Después de un contrato adjudicado, la alta gerencia tendrá que llevar a cabo pruebas y procedimientos de aceptación. El auditor deberá asegurarse de que la planificación de la prueba se lleva a cabo con suficiente antelación para que los requisitos de prueba se incluyan en el contrato.

En la evaluación de la fase de post implementación, el auditor deberá asegurarse de que la alta gerencia no ha aceptado equipos o software que no cumpla con sus exigencias.

El contrato debe especificar las condiciones aceptables para rendimiento. Por ejemplo, el contrato podrá exigir que una computadora funcionando con éxito durante 30 días consecutivos de un período de prueba de 90 días. El personal de la Agencia debe garantizar que el contratista cumpla plenamente las condiciones para un rendimiento aceptable. Los auditores internos pueden ser necesarios para verificar que el equipo o programa informático pase las pruebas especificadas.

La evaluación de la fase de prueba y la aceptación puede requerir un alto nivel de conocimientos técnicos por parte de los auditores, por ejemplo, cuando la alta gerencia ha contratado los servicios de desarrollo de software y debe poner a prueba la calidad de entrega de éste. El auditor debe ser capaz de entender los requisitos del sistema, desarrollo de metodologías y herramientas de prueba que se esté utilizando.

11.9.1 Objetivos de Auditoria

Confirmar que la alta gerencia cuenta con:

1. La definición de sus requisitos para las pruebas de la la tecnología que se puede comprar.
2. Que se Lleven realmente a cabo los procedimientos de prueba y aceptación para verificar que los recursos adquiridos satisfacen las necesidades de la alta gerencia.

11.9.2 Documentación Requerida

- Requisitos para la presentación de informes de costos y el estado dela gestión de configuración y supervisión de la gestión.
- Los registros de los exámenes de configuración u otros informes progreso.
- informes de problemas u otros registros de las deficiencias detectadas por el personal de la alta gerencia.
- Actas de aceptación de productos.
- Prueba de planes para la inspección y aceptación.

11.9.3 Pasos de Auditoria

1. Determinar si los planes de prueba se han desarrollado para determinar :

a. Las satisfacción de los requisitos funcionales

b. Los requisitos de seguridad derivados de la política gubernamental, las necesidades de la alta gerencia, y las necesidades específicas del usuario se mostraron satisfechos.

2. Determinar si los planes de prueba incluyen:

a. Tipos de pruebas

- La prueba de unidad-por ejemplo, en software, módulos de código se prueban por el programador que lo escribió.
- Pruebas integradas, por ejemplo, en el software, las funciones de agregado formado por grupos de módulos y enlaces de intermódulos de comunicación se ponen a prueba.
- Las pruebas examinan el funcionamiento del sistema como una entidad en un entorno operativo real o simulado.

a. Los lugares para la prueba.
b. Un programa de pruebas realistas.
c. Las necesidades de recursos

- Equipo de prueba necesaria, incluido el período de uso específico, tipos y cantidades necesarias.

- Software necesario para apoyar la prueba.

- El personal de usuario y grupos de adquisición con los números necesarios y las habilidades especificadas.

d. Materiales de prueba a ser usado

- Documentación necesaria, como el código fuente y manuales.
- Software para ser probado y su medio.
- Prueba de las entradas y salidas de la muestra.
- Prueba de software de control y hojas de cálculo.

e. Capacitación al personal en las pruebas a realizarse.

3. Determinar si se han establecido criterios para la certificación de que los requisitos de seguridad se cumplan.

4. Determine si el representante de los usuarios apropiados ha reconocido oficialmente la realización de las pruebas y la aceptación del sistema. Si no, determinar las razones y el impacto potencial.

a. Determine si las deficiencias descubiertas en las prestaciones del contrato se resolverá con rapidez.

b. Determinar si los requisitos que no fueron recibidos por el hardware suministrado, el software y las telecomunicaciones siguen pendientes y por qué.

5. Entrevista a los operadores de los sistemas y usuarios para determinar si el sistema ha sido integrado con éxito en el entorno existente.

11.9.4. CobiT Recomienda…

- Confirme que los principales interesados son considerados en las actividades de prueba de aceptación final.
- Averiguar si, y confirme que en las etapas de recepción definitiva, los criterios de éxito son identificados en el plan de pruebas.
- Averiguar si, y confirme que la documentación apropiada para su revisión y evaluación existe.
- Infórmese a las partes interesadas, que la documentación y presentación de los resultados finales de las pruebas de aceptación están completos y son oportunos.

12. CONCLUSIONES

Visto globalmente el proceso de adquisición en las organizaciones, estas manejan un alto grado de porcentaje de error o fracaso a la hora de realizar un proyecto de adquisición, ya que por lo general no tienen un proceso de gestión para el mismo. Suelen gestionar la selección del proveedor, y demás tareas del proceso de adquisición con una mezcla de suerte e intuición.

Debido a la competencia que existe en el mercado informático el beneficio es alto a la hora de buscar software que responda a determinadas expectativas en las organizaciones, sin embargo, el reto y objetivo es saber hacer una selección adecuada del posible proveedor; una evaluación concienzuda basada en las necesidades y requerimientos reales de la organización; una fase de pruebas donde no se sacrifique la imagen del producto, la calidad del mismo y el tiempo de salir a producción, y por último en una buena campaña de divulgación y capacitación.

Se identificó que la participación de la Gerencia y de cada uno de los usuarios directos que interactúan con todos y cada uno de los procesos en la organización y sobre todo con el proceso implicado directamente con la adquisición son de vital importancia a la hora de hallar los requerimientos de información, que son base fundamental para una óptima adquisición.

La atención que se le preste a la interacción entre la parte humana –usuarios -, el mercado y las necesidades emergentes cada día es la garantía para llevar a buenos términos el proceso de adquisición.

Hay que tener en cuanta a elementos claves como Infraestructura: cableado estructurado, equipos de interconectividad, servidores; y elementos lógicos entre

otros. Sistema operativo, Aplicaciones y sistemas de información. Adicional a la infraestructura se debe tener en cuenta las necesidades funcionales y no funcionales; el presupuesto y tiempo en que debe entrar a producción la nueva adquisición.

Para facilitar dicha tarea se puede recurrir a la Guía Metodológica enunciada en este documento, ya sea para toda la organización o para departamentos dentro de la misma.

Sin embargo, nunca dejará de existir controversia al momento de adquirir una nueva herramienta computacional en cualquier organización; Ya que obviamente van a existir puntos de vista diferentes a la hora de la selección y de la toma de decisiones.

13. BILBIOGRAFÍA

[1] http://www.gao.gov/ (Siendo Miembro)

[2] A Comparison of Internal Controls: COBIT®, SAC, COSO and SAS 55/78 By: Janet L. Colbert, Ph.D., CPA, CIA and Paul L. Bowen, Ph.D., CPA. http://www.isaca.org/bkr_cbt3.htm 26-06-2002 4:50 p.m.

[3] Information Systmes audit and Control Association. http://www.isaca.org/isacafx.htm. Junio 6 de 2002- 8:58.

[4] http://gfranklin.iespana.es/tesis/resumentot.pdf

[5] **Documento**: http://iteso.mx/~dlizalde/software.htm
Portal: http://portal.iteso.mx/portal/page/portal/ITESO

[6] Teoría de Administración de riegos- Néstor Orlando Romero ABCP,Msc-Mayo 2002.

[7] http://www.gestiopolis.com/delta/term/TER343.html
La Cadena de Valor y el Conocimiento Organizacional en la sociedad del conocimiento.

[8] http://www.gestiondelconocimiento.com/documentos2/caridad/cadena.htm

[9] R. Singh, "International Standard ISO/IEC 12207 Software Life Cycle Processes," Federa Aviation Administration, 1995.

[10] Organization for Standardization/International Electrotechnical Commission, "International Standard ISO/IEC 15504 Software Process Improvement and Capability Determination," 2004.

[11] Dodson K., Hofmann H., Ramani G. et al., Adapting CMMI for Acquisition Organizations: A Preliminary Report, CMU/SEI-2006-SR-005, Software Engineering Institute, 2006.

[12] ITSqc Carnegie Mellon, "eSCM-CL v1.1, Part 1," 2006.

ANEXOS

ANEXO A: ENCUESTA

ENCUESTA PARA EL CONOCIMIENTO DEL NIVEL DE GESTIÓN DE DISEÑO, PLANEACIÓN Y EJECUCIÓN DEL PROCESO DE ADQUISICIÓN DE SOFTWARE

La siguiente encuesta se realizará con el fin de obtener resultados a cerca del índice de la planeación, diseño y uso de metodologías de gestión de adquisición

Conteste SI o NO a las siguientes preguntas:

No.	Pregunta	SI	NO	Comentario
1	¿Existen estrategias definidas para la gestión de proyectos en la organización?			
2	¿Se manejan indicadores de nivel de definición de las estrategias planificadas?			
3	¿El proceso de gestión de riesgos de adquisición de software es parte de la gestión de proyectos definida?			
4	¿Está documentado y definido el proceso de gestión y planificación de proyectos de compra de software?			
5	¿Cuando se llevan a cabo los proyectos de compra de software se cumplen los plazos estimados?			
6	¿Los proyectos de compra son gestionados siguiendo un procedimiento establecido?			
7	¿Se identifican los riesgos para cada uno de los proyectos de compra de software?			
8	¿Existe un mecanismo establecido para analizar los riesgos de compra de software?			
9	¿Existen planes para mitigación, supervisión y control de riesgos en los proyectos de compra de software?			
10	¿Utilizaría un modelo que ayude a definir los procesos de gestión de proyectos de compra de software?			
11	¿Estaría dispuesto a implementar otra metodología para el proceso de gestión de riesgo en un proyecto de compra de software?			
12	¿Los resultados de la metodología de gestión de riesgos serían tenidos en cuenta durante el desarrollo de proyectos de compra?			

ANEXO B: LISTA DE CHEQUEO

LISTA DE CHEQUEO	SI	NO	N/A
ADMINISTRACION Y SOPORTE A USUARIO			
1. ¿Existe apoyo por parte de la gerencia en el proceso de adquisición?			
2. ¿La responsabilidad del proyecto de adquisición esta en mano de los directivos?			
3. ¿La gerencia está incluida a lo largo de todo el proceso de adquisición?			
4. ¿Los usuarios finales participan a lo largo de todo el proceso de adquisición?			
5. ¿Los pales y objetivos de la adquisición han sido aprobados y analizados por la alta gerencia?			
6. ¿El presupuesto del proceso de adquisición ha sido aprobado por la alta gerencia?			
7. ¿Los roles de los usuarios han sido asignados?			
8. ¿Los responsables del proceso están identificados?			
9. ¿Está bien definido el objetivo de la adquisición?			
10. ¿Han sido aprobadas las metas y objetivos de la adquisición?			
11. ¿Existe patrocinador o sponsor del proyecto?			
12. ¿Existe un proceso formal para mantener informada a todas las partes de cualquier cambio?			
13. ¿Existen fondos iniciales para el proyecto?			

LISTA DE CHEQUEO	SI	NO	N/A
14. ¿Existen funcionarios encargados de la seguridad de los controles internos en el proyecto?			
15. ¿Existen reglamentos o procedimientos para determinar las funciones o roles asignados a los usuarios?			
16. ¿Los usuarios participan en las revisiones periódicas?			
17. ¿Están asignados los recursos necesarios para la elaboración del proyecto?			
18. ¿Existe conciencia y conocimiento del proceso por parte de los usuarios?			
PERSONAL IMPLICADO EN EL PROYECTO			
19. ¿Existe un gerente de proyecto?			
20. ¿Están claramente asignados los roles funciones y responsabilidades?			
21. ¿Existe personal experto en el proceso?			
22. ¿Existe una lista de miembros del equipo con sus respectivas responsabilidades en el proyecto?			
23. ¿Esta claramente definida la responsabilidad del administrador del proyecto?			
24. ¿El administrador del proyecto ha realizado anteriormente proyectos similares?			
25. ¿La combinación de las habilidades del personal son adecuadas?			
26. ¿El personal implicado en el proyecto tiene experiencia en administración de contratistas?			
27. ¿El personal del proyecto ha sido capacitado para mantener su competencia?			

LISTA DE CHEQUEO	SI	NO	N/A
NECESIDADES, REQUERIMIENTOS Y ESPECIFICACIONES			
28. ¿Están claramente definidos las necesidades de información del proyecto?			
29. ¿Existe un plan para la identificación de necesidades y recursos de información que se necesitan en el proyecto?			
30. ¿Los requisitos de tecnología son claros y precisos?			
31. ¿El hardware y software necesario ha sido identificado claramente?			
32. ¿La adquisición se basa en las necesidades y oportunidades y son coherentes con la estrategia y arquitecturas utilizadas por la organización?			
33. ¿Las necesidades de la gerencia están basadas en las necesidades identificadas previamente por los usuarios?			
34. ¿Las necesidades identificadas apoyan la adquisición de hardware software y telecomunicaciones?			
35. ¿Existe un plan de pruebas anterior a la adjudicación del contrato?			
36. ¿La alta dirección personal de proyecto y los usuarios están de acuerdo con la identificación de las necesidades, análisis y requerimientos?			
37. ¿La alta gerencia tiene definidas sus funciones y necesidades de apoyo?			
38. ¿Esta identificado si la tecnología que se va a adquirir cumple con las normas gubernamentales?			
39. ¿Existe compatibilidad entre lo que se va a adquirir y lo que se tiene?			

LISTA DE CHEQUEO	SI	NO	N/A
40. ¿Esta identificado quien es el responsable de revisar y aprobar cambios?			
41. ¿Los usuarios finales y el director de programa confirmaron que las especificaciones reflejan con precisión los requisitos o requerimientos y se ajustan al proceso de adquisición?			
42. ¿Los requerimientos han sido aprobados y firmados por la alta dirección?			
43. ¿Están identificadas las funciones que debe cumplir el software?			
44. ¿Existe soporte y mantenimiento del sistema de aplicación?			
45. ¿Existen manuales de procedimiento?			
46. ¿Existen manuales de usuario?			
47. ¿Existen ayudas en línea?			
48. ¿Las operaciones del personal de apoyo están involucradas en el desarrollo y mantenimiento de las operaciones y la documentación de apoyo?			
49. ¿Los cambios son monitoreados revisados y aprobados?			
50. ¿Los cambios realizados son registrados en el sistema de gestión de cambios?			
51. ¿Los cambios son comunicados a todo el personal?			
ALTERNATIVAS			
52. ¿Se han considerado todas las alternativas razonables para cubrir las necesidades?			

LISTA DE CHEQUEO	SI	NO	N/A
53. ¿Se han identificado los riesgos, costos y beneficios de cada alternativa?			
54. ¿Se han realizado los análisis económicos y de riesgos de cada alternativa?			
55. ¿Se han realizado estudios de mercado para identificar alternativas?			
56. ¿Se han hecho estudios de costo beneficio para justificar la elección de la alternativa?			
57. ¿Existe una adecuada administración por parte de quien aprobó a alternativa seleccionada?			
58. ¿Los directivo y el personal de contratación participar en el análisis de alternativas?			
59. ¿Se analizaron todas las alternativas teniendo en cuenta los mismos criterios de evaluación?			
60. ¿Las alternativas fueron descritas detalladamente?			
61. ¿La alternativa considerada cubre la arquitectura de información de la alta gerencia?			
62. ¿Todas las alternativas fueron consideradas en el presupuesto de los recursos?			
63. ¿Cada análisis de las alternativas incluyen un análisis de sensibilidad para identificar los factores que afectan la elección de una alternativa sobre las otras?			
64. ¿Se hizo un análisis de riesgos para identificar datos sensibles y vulnerables?			
65. ¿Se hizo un análisis de la magnitud de la vulnerabilidad identificada?			
66. ¿Se evaluaron los riesgos técnicos y financieros de cada			

LISTA DE CHEQUEO	SI	NO	N/A
alternativa?			
67. ¿La alternativa cumple con los requisitos legislativos?			
68. ¿La adquisición incluye y hace cumplir los derechos y obligaciones de todas las partes?			
69. ¿El asesoramiento jurídico ha tenido en cuenta la parte de concesión de licencias de propiedad intelectual?			
70. ¿Los acuerdos de adquisición son identificados?			
71. ¿Los acuerdos cumplen con las políticas de la empresa?			
72. ¿La adquisición es revisada y aprobada por el personal apropiado y con el asesoramiento jurídico necesario?			
73. ¿Los contratos son revisados y aprobados?			
74. ¿Los derechos y obligaciones de todas las partes son evaluados en el proceso de adquisición?			
75. ¿Las adquisiciones e hardware y software son registradas?			
76. ¿La organización se asegura de que el producto adquirido cumple los requisitos de compra especificado?			
77. ¿La información de las compras describe el producto a comprar, incluyendo, cuando sea apropiado: • Requisitos para la aprobación del producto, procedimientos, procesos y equipos, • Requisitos para la calificación del personal, y • Requisitos del S.G.C.?			
78. ¿La organización debe asegurarse de la adecuación de los requisitos de compra especificados antes de comunicárselos al proveedor. ?			

LISTA DE CHEQUEO	SI	NO	N/A
79. ¿La organización debe establecer e implementar la inspección u otras actividades necesarias para asegurarse de que el producto comprado cumple los requisitos de compra especificados?			
80. ¿Cuando la organización o su cliente quieran llevar a cabo la verificación en las instalaciones del proveedor, la organización debe establecer en la información de compra las disposiciones para la verificación pretendida y el método para la liberación del producto?			
81. ¿La alta gerencia evalúa y selecciona los proveedores en función de su capacidad de acuerdo a los requisitos de la organización?			
82. ¿Están establecidos los criterios para la selección, evaluación y re-evaluación?			
PLAN DE ADQUISICIÓN			
83. ¿La alta gerencia contempla dentro del plan de adquisición una estrategia global para el proceso?			
84. ¿El plan de adquisición especifica el tipo de contrato que será adjudicado?			
85. ¿El plan de adquisición es realista y completo?			
86. ¿Existe dentro del plan de adquisición un plan de acción y metas?			
87. El plan de adquisición fue revisado y aprobado de manera oportuna por los funcionarios designados por la alta gerencia?			
88. ¿El plan de adquisición identifica el método de adquisición el plan de capacitación formal y un plan de contingencia para minimizar las perdidas?			

LISTA DE CHEQUEO	SI	NO	N/A
89. ¿Existe una organización por módulos en el plan de adquisición?			
90. ¿Existe en el proceso de adquisición una selección total y abierta del proveedor?			
91. ¿Existe una técnica de proyectos para satisfacer los requisitos de gestión de información?			
92. ¿Existe una lista de recursos tecnológicos utilizados actualmente?			
DOCUMENTO DE LICITACIÓN			
93. ¿La licitación proporciona información necesaria para ofrecer equipos software y servicios?			
94. ¿Las propuestas de los proveedores son precedidas por una solicitud de información o cotización?			
95. ¿La solicitud de la propuesta es clara y concreta?			
96. ¿La a organización ha tomado medidas para garantizar del contratista son competitivas?			
97. ¿La propuesta es exacta y describe claramente los requisitos de la organización?			
98. ¿La propuesta es restrictiva, o sea favorece a uno de los contratistas sobre los demás?			
99. ¿Los auditores son suficientemente conocedores de la auditoria de la información?			
SELECCIÓN DE RECURSOS			
100. ¿El proceso de evaluación se ajusta a la solicitud de oferta de la alta gerencia?			
101. ¿La gerencia evalúa la parte técnica de las diferentes			

LISTA DE CHEQUEO	SI	NO	N/A
propuestas?			
102. ¿El proceso de selección es planificado para llevar a cabo el éxito del contrato?			
103. ¿Existe un informe en el que se describe las negociaciones y las actividades de selección?			
104. ¿Existe una propuesta de guía de evaluación?			
105. ¿Existen revisiones pre auditoria?			
106. ¿La documentación de controles e revisada para proteger la seguridad de información confidencial?			
107. ¿Los costos estimados del ciclo de vida concilian con la propuesta del proveedor?			
108. ¿Los informes finales fueron documentados?			
GESTIÓN DE CONTRATOS			
109. ¿La Alta Gerencia Realiza La Vigilancia Al Desempeño Del Contratista?			
110. ¿La alta gerencia lleva a cabo reseñas de postimplementacion?			
111. ¿La alta gerencia asegura que los requisitos del contrato continuarán reflejando con precisión las necesidades de los usuarios?			
112. ¿La alta gerencia verifica que los productos y servicios entregados cumplen las necesidades de los usuarios?			
113. ¿La alta gerencia modifica el contrato solo cuando es necesario?			
114. ¿La alta gerencia aplica las disposiciones del contrato destinado a proteger la alta gerencia, tales como garantías o			

LISTA DE CHEQUEO	SI	NO	N/A
daños y perjuicios? **115.**			
116. ¿Existe documentación del contrato adjudicados con las modificaciones si estas existieran?			
117. ¿Existe documentación del presupuesto actual?			
118. ¿Existe documentación del plan de gestión para la configuración del proyecto?			
119. ¿Los usuarios y los altos directivos están implicados en la gestión del contrato y la aprobación de cualquier cambio?			
120. ¿Existe una evaluación del personal del proyecto?			
121. ¿El contrato refleja las necesidades de los usuarios?			
122. ¿Existe un proceso de revisión para garantizar que cambios propuestos de ingeniería están dentro del alcance del contrato? **123.**			
PRUEBA Y ACEPTACIÓN			
124. ¿El equipo adquirido cumplen con las necesidades del usuario y satisfacen los requisitos de seguridad?			
125. ¿La alta gerencia lleva a cabo pruebas y procedimientos de aceptación?			
126. ¿El contrato especifica las condiciones aceptables para el rendimiento de software?			
127. ¿La alta gerencia cuenta con la definición de sus requisitos para las pruebas de la tecnología que se puede comprar?			

LISTA DE CHEQUEO	SI	NO	N/A
128. ¿Existe documentación de informes de problemas u otros registros de las deficiencias detectadas por el personal de la alta gerencia?			
129. ¿Existen actas de aceptación de productos?			
130. ¿Existen documentación de pruebas de planes para la inspección y aceptación?			
131. ¿El plan de pruebas satisface los requisitos funcionales?			
132. ¿Las pruebas examinan el funcionamiento del sistema como una entidad en un entorno operativo real?			
133. ¿Las pruebas examinan el funcionamiento del sistema como una entidad en un entorno operativo simulado?			
134. ¿Existen equipos y software necesario para la realización de las pruebas?			
135. ¿Existe documentación necesaria como código fuente y manuales?			
136. ¿Existe capacitación del personal?			
137. ¿se han establecido criterios para la certificación de que los requisitos de seguridad se cumplan?			
138. ¿se han realizado entrevistas a los operadores de los sistemas y usuarios para determinar si el sistema ha sido integrado con éxito en el entorno existente?			

ANEXO C: CESIÓN DE DERECHOS DE AUTOR

Corporación Universitaria de la Costa

CESIÓN DERECHOS DE AUTOR DEL TRABAJO DE GRADO

A FAVOR DE LA CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC

Yo, Mario Orozco Bohórquez, manifiesto en este documento mi voluntad de ceder a la Corporación Universitaria de la Costa los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982, del trabajo final de grado denominado GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO, producto de mi actividad académica para optar el título de Especialista en Auditoria de Sistemas de Información en la Corporación Universitaria de la Costa, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y publicación. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento en el momento mismo que hago entrega del trabajo final a la Biblioteca Central de la Corporación Universitaria de la Costa, CUC.

Mario Orozco Bohórquez C.C. # 72.208.501 _____

NOMBRE CÉDULA FIRMA

Barranquilla, D.E.I.P., a los 21 días del mes de _Octubre_ de 2010.

"Los derechos de autor recaen sobre las obras científicas, literarias y artísticas en las cuales se comprenden las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación, tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantonimias; las composiciones musicales con letra o sin ella; las obras cinematográficas a las cuáles se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los videogramas, las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresas por procedimiento análogo o la fotografía; las obras de artes plásticas; las ilustraciones, mapas, planos, croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias, en fin, toda producción del dominio científico, literario o artístico que puedan producirse o definirse por cualquier forma de impresión o de reproducción, por fonografía o radiotelefonía o cualquier otro medio conocido o por conocer". (artículo 2 de la Ley 23 de 1982).

Corporación Universitaria de la Costa

CESIÓN DERECHOS DE AUTOR DEL TRABAJO DE GRADO

A FAVOR DE LA CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC

Yo, Ubaldo José Martínez Palacio, manifiesto en este documento mi voluntad de ceder a la Corporación Universitaria de la Costa los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982, del trabajo final de grado denominado GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO, producto de mi actividad académica para optar el título de Especialista en Auditoria de Sistemas de Información en la Corporación Universitaria de la Costa, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y publicación. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento en el momento mismo que hago entrega del trabajo final a la Biblioteca Central de la Corporación Universitaria de la Costa, CUC.

Ubaldo José Martínez Palacio C.C. # 72.333.456 _____

NOMBRE CÉDULA FIRMA

Barranquilla, D.E.I.P., a los 21 días del mes de _Octubre_ de 2010.

"Los derechos de autor recaen sobre las obras científicas, literarias y artísticas en las cuales se comprenden las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación, tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantonimias; las composiciones musicales con letra o sin ella; las obras cinematográficas a las cuáles se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los videogramas, las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresas por procedimiento análogo o la fotografía; las obras de artes plásticas; las ilustraciones, mapas, planos, croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias, en fin, toda producción del dominio científico, literario o artístico que puedan producirse o definirse por cualquier forma de impresión o de reproducción, por fonografía o radiotelefonía o cualquier otro medio conocido o por conocer". (artículo 2 de la Ley 23 de 1982).

Corporación Universitaria de la Costa

CESIÓN DERECHOS DE AUTOR DEL TRABAJO DE GRADO

A FAVOR DE LA CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC

Yo, William Manuel Torres Royero, manifiesto en este documento mi voluntad de ceder a la Corporación Universitaria de la Costa los derechos patrimoniales, consagrados en el artículo 72 de la Ley 23 de 1982, del trabajo final de grado denominado GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO, producto de mi actividad académica para optar el título de Especialista en Auditoria de Sistemas de Información en la Corporación Universitaria de la Costa, entidad académica sin ánimo de lucro, queda por lo tanto facultada para ejercer plenamente los derechos anteriormente cedidos en su actividad ordinaria de investigación, docencia y publicación. La cesión otorgada se ajusta a lo que establece la Ley 23 de 1982. Con todo, en mi condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la Ley 23 de 1982. En concordancia suscribo este documento en el momento mismo que hago entrega del trabajo final a la Biblioteca Central de la Corporación Universitaria de la Costa, CUC.

William Manuel Torres Royero C.C. # 1045678854 _____

NOMBRE CÉDULA FIRMA

Barranquilla, D.E.I.P., a los 21 días del mes de _Octubre_ de 2010.

"Los derechos de autor recaen sobre las obras científicas, literarias y artísticas en las cuales se comprenden las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación, tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las

obras dramáticas o dramático-musicales; las obras coreográficas y las pantonimias; las composiciones musicales con letra o sin ella; las obras cinematográficas a las cuáles se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los videogramas, las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas a las cuales se asimilan las expresas por procedimiento análogo o la fotografía; las obras de artes plásticas; las ilustraciones, mapas, planos, croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias, en fin, toda producción del dominio científico, literario o artístico que puedan producirse o definirse por cualquier forma de impresión o de reproducción, por fonografía o radiotelefonía o cualquier otro medio conocido o por conocer". (artículo 2 de la Ley 23 de 1982).

ANEXO D: ENTREGA DEL TRABAJO DE GRADO Y AUTORIZACIÓN DE USO

Corporación Universitaria de la Costa

ENTREGA DEL TRABAJO DE GRADO Y

AUTORIZACIÓN DE SU USO A FAVOR DE LA

CORPORACIÓN UNIVERSITARIA DE LA COSTA

Yo, Mario Orozco Bohórquez, mayor de edad, identificado con la cédula de ciudadanía N° 72.208.501, de Barranquilla, actuando en nombre propio, en mi calidad de autor del trabajo de tesis, monografía o trabajo de grado denominado: GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO, hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD ROM) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento. PAARÁGRAFO: La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato virtual, electrónico, digital, óptico, usos en red, Internet, extranet, intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los _21_ días del mes de _Octubre_ de Dos Mil Diez_ 2010.

EL AUTOR - ESTUDIANTE.

(Firma).....

Nombre: Mario Orozco Bohórquez_____

C.C. N° _72.208.501_ de __Barranquilla__

Corporación Universitaria de la Costa

ENTREGA DEL TRABAJO DE GRADO Y

AUTORIZACIÓN DE SU USO A FAVOR DE LA

CORPORACIÓN UNIVERSITARIA DE LA COSTA

Yo, Ubaldo Jose Martínez Palacio, mayor de edad, identificado con la cédula de ciudadanía N° 72.333.456, de _Barranquilla_, actuando en nombre propio, en mi calidad de autor del trabajo de tesis, monografía o trabajo de grado denominado: GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO, hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD ROM) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento. PAARÁGRAFO: La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato virtual, electrónico, digital, óptico, usos en red, Internet, extranet, intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los _21_ días del mes de _Octubre_ de Dos Mil Diez_ 2010.

EL AUTOR - ESTUDIANTE.

(Firma).....

Nombre: Ubaldo Jose Martínez Palacio_

C.C. N° _72.333.456_ de __Barranquilla__

Corporación Universitaria de la Costa

ENTREGA DEL TRABAJO DE GRADO Y

AUTORIZACIÓN DE SU USO A FAVOR DE LA

CORPORACIÓN UNIVERSITARIA DE LA COSTA

Yo, William Manuel Torres Royero, mayor de edad, identificado con la cédula de ciudadanía N° 1045678854, de Barranquilla, actuando en nombre propio, en mi calidad de autor del trabajo de tesis, monografía o trabajo de grado denominado: GUIA METODOLOGICA DE ADQUISICION DE SOFTWARE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL SECTOR PRIVADO, hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD ROM) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento. PAARÁGRAFO: La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato virtual, electrónico, digital, óptico, usos en red, Internet, extranet, intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los _21_ días del mes de _Octubre_ de Dos Mil Diez_ 2010.

EL AUTOR - ESTUDIANTE.

(Firma).....

Nombre: William Manuel Torres Royero

C.C. N° _1045678854_ de __Barranquilla__

ANEXO E: MAPEO GAO, COBIT E ISO 9000

MAPPING: GAO - CobiT(Assegurance Guide) - ISO 9000

Information Technology: An Audit Guide for Assessing Acquisition Risks **Ítem # 1:** Administración y soporte al usuario		
Este capítulo se centra en los niveles de compromiso y apoyo para proyectos de adquisición para la alta dirección y los usuarios, dos stakeholders principales en el proceso de adquisición. Los altos directivos son los que tienen en general la responsabilidad por motivos estratégicos, incluyendo información relacionada con los objetivos. Los usuarios son los que en realidad operan los recursos de información de la empresa e incluyen a la dirección para establecer políticas institucionales y para los programas apoyados por la adquisición. La participación y el apoyo de la gerencia a lo largo de un proceso de adquisición son esenciales para el éxito.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: ➢ Asegurarse de que la alta gerencia brinde apoyo y participe activamente en todo el desarrollo y aplicación del proceso de adquisición. ➢ Garantice que los usuarios participen activamente en el proceso de adquisición y en la definición de las necesidades, desarrollando el documento de solicitud de requerimientos y verificando que los equipos y / o servicios contratados satisfacen las necesidades de la	➢ Entrevista con personal clave acerca de crear la conciencia en el grupo de usuarios y el conocimiento de los proceso para que el uso del sistema se haga de una manera eficaz y eficiente usando los sistemas de aplicación que soportan los procesos del negocio. (por ejemplo, la formación y desarrollo de capacidades, materiales de capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, soporte de mesa de	

organización. **Documentación:** ➢ Los Documentos, memorandos, u otros registros de la gerencia deben ser analizados y aprobados en los planes y objetivos de adquisición. ➢ La Gerencia de administración de programa u altos directivos que indicando objetivos y objetivos de la adquisición y la delegación de autoridad para llevar a cabo la adquisición. ➢ El Presupuesto y planos que indican la financiación del proyecto deben estar contemplados en el proceso de adquisición. **Pasos de la Auditoría:** ➢ Apoyo de la Alta Dirección ➢ Participación de los usuarios	servicio, la identificación del usuario clave, evaluación). ➢ Revisión de formación y materiales de aplicación para determinar si el proceso definido, incluye el contenido requerido. ➢ Confirmar a través de entrevistas con miembros clave que el usuario es consciente y capaz de utilizar el mecanismo de retroalimentación para evaluar la adecuación de la documentación de apoyo, procedimientos y capacitación relacionada.	

Information Technology: An Audit Guide for Assessing Acquisition Risks **Ítem # 2:** Administración y soporte al usuario		
Al personal del proyecto de adquisición se le debe asignar muy claramente sus roles, funciones y responsabilidades. El equipo debe incluir miembros que son expertos en la información proceso de adquisición de tecnología, entender la tecnología y tener experiencia en la administración de contratos. El equipo también deberá tener miembros con conocimientos sobre los programas que la adquisición apoyará.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivo: ➢ Determinar si el equipo de adquisición tiene las habilidades necesarias y la autoridad para planificar eficazmente y ejecutar el proyecto. **Documentación:** ➢ Una lista de los principales miembros del equipo del proyecto mostrando sus responsabilidades, cargos, y la experiencia. El auditor puede generar esa lista sobre la base de las entrevistas si alguno de ellos no está disponible. ➢ La solicitud de contratación para que una delegación de facultades de adquisición de GSA, mostrar los nombres y experiencia de los funcionarios de proyecto		

Pasos de la Auditoría: ➢ Administración del Proyecto ➢ Personal del proyecto		
Information Technology: An Audit Guide For Assessing Acquisition Risks **Ítem** # 3**:** Necesidades / Requerimientos / Especificaciones		
El propósito de este capítulo es orientar al auditor en determinar si la Alta Gerencia ha desarrollado una descripción precisa de su tecnología, información y necesidades. La adquisición debe estar claramente vinculadas al las necesidades del programa, a las estrategias generales de la Alta Gerencia, y el gobierno en cuanto a políticas y normas.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: ➢ Garantizar que la adquisición se basa claramente en las necesidades, oportunidades y que es coherente con la estrategia global y arquitecturas utilizadas por el organismo. ➢ Asegurar que la Alta Gerencia define sus necesidades, basadas en las necesidades previamente identificadas y validadas por usuarios funcionales, lo suficiente como para apoyar la adquisición de hardware, software, telecomunicaciones, y	➢ Entrevista con miembros claves sobre la conciencia del personal de soporte técnico y operaciones y el conocimiento del proceso de manera eficaz y eficiente, soporte y mantenimiento del sistema de aplicación y la correspondiente infraestructura de acuerdo a los niveles de servicio (por ejemplo, la formación y desarrollo de capacidades, materiales de capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, los escenarios de servicios de escritorio). ➢ Revisión formación y materiales de implementación para determinar si el proceso definido, incluye el	

sistema servicios de desarrollo. Estos requisitos deben ante todo ser expresados en términos funcionales de acuerdo con la política **FIRMR**. ➢ Garantizar claridad en las especificaciones del sistema y precisión en el resumen de especificaciones de la Alta Gerencia. **Documentación:** ➢ Declaración de necesidades. ➢ Análisis de requerimientos o documento de requisitos funcionales ➢ Especificaciones del sistema, si se han preparado. También, proyecto de especificaciones con comentarios de la industria si las especificaciones del proyecto fueron liberados. ➢ Plan de pruebas y requisitos antes de la adjudicación del contrato. Requisitos de ensayo puede resumirse en una prueba y evaluación del plan maestro.	contenido requerido. ➢ Confirmar a través de entrevistas con miembros clave del personal que el personal de soporte técnico y de operaciones es consciente y capaz de utilizar el mecanismo de retroalimentación para evaluar la adecuación de la documentación de apoyo, procedimientos y capacitación relacionada. ➢ Determinar si las operaciones y personal de apoyo están involucrados en el desarrollo y mantenimiento de las operaciones y la documentación de apoyo. ➢ Identificar las áreas donde los procedimientos de soporte operacionales no están integrados con los procedimientos de soporte operacional. ➢ Asegurar y confirmar que los cambios en las necesidades individuales son monitoreados, revisados y aprobados por los actores involucrados. ➢ Inspeccione la documentación pertinente para confirmar que todos los cambios y el estado de cambios se registran en el sistema de gestión del cambio.	

Pasos de la Auditoría: ➢ Determinación de Necesidades ➢ Requerimientos Análisis ➢ Especificaciones ➢ Planes de Evaluación	➢ Identificar y comunicar los cambios a los que no se realiza un seguimiento.	

Information Technology: An Audit Guide For Assessing Acquisition Risks **Ítem # 4:** Alternativas
Después de identificar sus necesidades, la empresa debe evaluar las **alternativas** para examinar el costo-beneficio de dichos requisitos. La alternativa seleccionada, debe reflejar una comprensión de lo que está disponible tanto en el mercado comercial, como en el gobierno. Analizando cómo dicha alternativa apoya en el proceso de adquisición se reducen, pero no elimina, el riesgo de que otra compañía pueda seleccionar una alternativa que no satisfaga plenamente a los usuarios sus necesidades, u otras que sean innecesarias, complejas y de alto costo.

A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: ➢ Determinar si la Alta Gerencia ha considerado todos alternativas razonables para cubrir sus necesidades. ➢ Determinar si la Alta Gerencia	• Confirmar a través de entrevistas con miembros o personales clave que en el proceso de adquisición y planificación de la estrategia de adquisición de TI estén alineados con las políticas de contratación de la organización y procedimientos (**por ejemplo**, requisitos	➢ Que dentro de las opciones de solución que ofrece la **ISO 9000** con respecto a los problemas que generalmente influyen la mala gestión de Calidad está la **revisión** de la política de calidad documentada orientándola hacia la calidad, los clientes,

identifica los riesgos, los costos y beneficios de cada alternativa. ➢ Comprobar que la Alta Gerencia seleccionada presente una alternativa equilibrada de los beneficios previstos con relación a los costos, tiempo y riesgos de fracaso. **Documentación:** ➢ Registro de análisis de alternativas, como un documento de decisión del sistema. Los análisis económicos y de riesgo deben acompañar o ser parte del documento de decisión. ➢ Encuesta con estudios de mercado llevada a cabo para identificar alternativas para las necesidades del usuario de reuniones y para	legislativos, el cumplimiento de la organización de TI de la adquisición de la política, las licencias y los requisitos de arrendamiento, las cláusulas de actualización tecnológica, participación de la empresa, costo total de propiedad, el plan de adquisición de grandes adquisiciones y por último el registro de los activos). • Revise las políticas de gestión y procedimientos de los proyectos para evaluar la conformidad con las políticas de contratación y los procedimientos de la empresa. • Confirmar a través de entrevistas con miembros clave del personal que las políticas y normas dan lugar para el establecimiento de contratos con los proveedores. Las políticas y normas que debe abordar, las responsabilidades del cliente-proveedor, proveedor **SLA**, control e información contra la **SLA**, disposiciones transitorias, los procedimientos de notificación y la progresividad, las normas de seguridad, los requisitos de	**proveedores** y mejoramiento continuo, realizando su ajuste. Así mismo partiendo de esta política de calidad que existía se subdividió para identificar de acuerdo a los objetivos de calidad, con los cuales debían trabajar todos los procesos de la entidad y sus colaboradores. Dentro de los principios de calidad, son el pilar de un S.G.C. cualquiera que sea su clase, una empresa que implemente estos principios está cumpliendo con cualquier norma certificable, dentro de los 8 principios que existen, nos interesa el No. 8 que es: **“Relaciones Mutuamente Beneficiosas con el Proveedor”**. ➢ Por último en la sesión **7.4** de los requerimientos que exige esta norma **ISO de calidad** es la

apoyar las estimaciones de costos. ➢ Las conclusiones y declaraciones de apoyo a la aprobación de restricciones a las especificaciones, tales como limitación de los requisitos de compatibilidad. ➢ El costo / beneficio para justificar la selección de la alternativa seleccionada frente a otras alternativas, en términos de dólares o en términos de otros criterios, tales como la eficacia.	gestión de registros y control, y requiere prácticas de los proveedores de control de calidad. Los contratos deben incluir también una parte jurídica, financiera, documental de organización, funcionamiento, seguridad, auditabilidad, la propiedad intelectual, la responsabilidad y los aspectos de sus asistencias • Confirmar a través de entrevistas con el personal clave con criterios predefinidos, específicos y establecidos (**por ejemplo**, la definición de los requisitos, calendario, proceso de decisión) se utilizan para la selección de proveedores y adquisición. • Inspeccione las solicitudes de información (**RFI**) y solicitudes de propuesta (**RFP**) para determinar si los criterios establecidos se definen.	llamada: **"Compras"**. Esta sesión menciona **3 incisos** que hablan del proceso de **compras** como tal, la información requerida y para realizar un buen trabajo de compras, se menciona los aspectos de la verificación de lo comprado. A continuación se citan los 3 puntos que son muy importantes a la hora de una adquisición de un producto y/o servicio (en este caso de estudio, **Adquisición de software**). **7.4.1** Proceso de compras **7.4.2** Información de las compras **7.4.3** Verificación de los productos comprados

Information Technology: An Audit Guide For Assessing Acquisition Risks **Ítem # 5:** Plan de Adquisición		
Para asegurar que la planificación se lleva a cabo de manera eficaz, económica y oportuna, la Alta Gerencia deberá preparar un plan de adquisición que contenga una estrategia global para la gestión de la aprobación previa, la adquisición, y las fases posteriores de adjudicación. Un plan de adquisición efectivo, es crítico para el éxito del proyecto. El plan establece lo que la Alta Gerencia va a hacer para completar una compra y cómo lo hará. El plan también especifica el tipo de contrato que será adjudicado, cómo la Alta Gerencia seleccionará un contratista, costo y el cronograma de metas, hitos, áreas importantes de riesgo y los controles de gestión de contratos.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: Comprobar que la Alta Gerencia ha definido una estrategia efectiva y un plan para la selección de un contratista y la gestión de la ejecución del contrato. **Documentación:** ➢ Plan de Adquisición y los documentos relacionados a su caso, como un plan de acción y metas. ➢ Solicitud de la Alta Gerencia de adquisición y otro tipo de correspondencia con la GSA.	➢ Confirme con el personal el plan para la adquisición, aplicación y/o actualización de la infraestructura de tecnología se ha creado el negocio que satisfaga requisitos funcionales y técnicos. ➢ Revisar el plan para confirmar que cumpla con la dirección tecnológica de la organización establecida y que todos los aspectos clave se incluyen. ➢ Averiguar si y confirmar que un proceso se ha definido e implementado para crear y mantener un plan de adquisición de	

	infraestructura que está alineado con el organización de la dirección tecnológica. ➢ Inspeccione el plan de adquisición de infraestructura para identificar las áreas en aspectos clave, tales como los requisitos, los riesgos, la transición y la migración, no se han abordado. ➢ Revisión de la evaluación financiera para la exactitud y la cobertura global	

Information Technology: An Audit Guide For Assessing Acquisition Risks

Ítem # 6: Documento de Licitación

Un documento de licitación proporciona información necesaria a los vendedores para proponer equipos, software y servicios para satisfacer los requisitos o requerimientos de la organización. En la mayoría de los casos, los recursos de información se adquirirán mediante la emisión de una solicitud de propuesta, que constituye la base para el contrato resultante. Con menos frecuencia, una organización podrá adquirir los recursos de información mediante una invitación a presentar ofertas. Una solicitud de propuesta puede ser precedida por una solicitud de información o solicitud de cotización.

Una solicitud de propuesta debe ser clara y completa, incluirá los elementos descritos en las directrices de la GSA en el documento estándar de licitación.

A tener en cuenta…	CobiT (Guías de Aseguramiento) Recomienda…	ISO 9000 Recomienda…
Objetivo: Determinar si el documento de licitación esta completo, clara y coherente. Compruebe que los requerimientos siguen reflejando las necesidades del usuario, y determine si el proceso de evaluación propuesto da lugar a una adquisición eficaz y económica. **Documentación:** ➢ Registro de la pre solicitud o propuesta preliminar. ➢ Documento de Solicitud: solicitud de propuesta o invitación para la oferta. ➢ Informe de un comité de revisión de solicitud o de una comisión, si es apropiado. ➢ Plan de selección del recurso. ➢ Materiales de referencia o de otras capacidades y requerimientos de validación de rendimiento. ➢ Comentarios del proveedor o preguntas sobre el documento de solicitud. ➢ Guía de evaluación Propuesta.		

Information Technology: An Audit Guide For Assessing Acquisition Risks **Ítem # 7:** Selección de Recursos		
El proceso de selección del recurso es crítico para asegurar el mejor valor para el gobierno. Todas las propuestas deben ser evaluadas de acuerdo a los criterios publicados en el **RFP**. Si el proceso de evaluación no se ajusta a la solicitud de ofertas de la Alta Gerencia, corre un riesgo mayor de que la respuesta de la oferta conlleve a la pérdida de los vendedores. La Alta Gerencia debe recibir las propuestas, evaluar la parte técnica y los méritos de las diferentes propuestas, negociar con los contratistas y adjudicar un contrato con arreglo a un plan de selección de fuente desarrollado antes de la liberación de la **RFP**.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: Garantizar que el proceso de selección de la fuente sea planificado y llevado a cabo para alcanzar con éxito un contrato que dé el mejor valor para el gobierno. **Documentación:** ➢ La selección de plan, incluyendo la selección de la organización base. ➢ Informe de las lecciones aprendidas u otro informe por el Funcionario contratante que describe		

las negociaciones y las actividades de selección. ➢ Archivo de contratación del Oficial de contrato. ➢ Los registros de reuniones informativas, si es pertinente. ➢ Resultados de los puntos de referencia o el rendimiento y otras técnicas de validación de la capacidad utilizada. ➢ La correspondencia entre los oferentes y la Alta Gerencia respecto a las preguntas o aclaraciones y cualquier enmienda a la RFP. ➢ Propuesta de guía de evaluación. ➢ Revisiones pre auditoría.		
Information Technology: An Audit Guide For Assessing Acquisition Risks **Ítem # 8:** Gestión de Contratos		
El contrato incluye la gestión de los pasos necesarios para asegurarse de que la Alta Gerencia recibe productos y servicios dentro de los costos y los plazos establecidos. Una Alta Gerencia tiene la obligación de vigilar el desempeño del contratista, garantizar que el trabajo realizado se ajusta a los requisitos de la Alta Gerencia. La misma, también debe controlar los cambios del contrato y aceptar o rechazar los resultados finales. Por último, una Alta Gerencia debe llevar a cabo Reseñas de post implementación para determinar qué tan bien objetivos de adquisición se cumplen y si los recursos de información adquiridos deben ser		

añadidos o sustituidos.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: Para asegurarse de que la Alta Gerencia: ➢ Supervisa el desempeño del contratista. ➢ Asegura que los requisitos del contrato continuará reflejan con precisión las necesidades de los usuarios. ➢ Verifica que los productos y servicios entregados cumplen necesidades de los usuarios. ➢ Realiza una gestión de configuración. Modifica el contrato sólo cuando sea necesario. ➢ Aplica las disposiciones del contrato destinado a proteger la Alta Gerencia, tales como garantías o daños y perjuicios cláusulas. **Documentación:** ➢ Alta Gerencia de reglamentos o directivas especificando requisitos para las revisiones periódicas, la gestión supervisión y administración de		

configuración. ➢ El contrato adjudicado y con las modificaciones. ➢ La organización de la Alta Gerencia de gestión de contratos y estructura. ➢ informes sobre la situación actual y el costo o el horario proyecciones. ➢ informes sobre el presupuesto actual. ➢ El plan de gestión de configuración para el proyecto.		
Information Technology: An Audit Guide For Assessing Acquisition Risks **Ítem # 9:** Prueba y Aceptación		
Las pruebas proporcionan la base para la toma de decisiones en cuanto a conveniencia de contratos se refiere. Para la obtener eficacia en la realización de pruebas estas deben ser dirigidas relativamente al proceso de adquisición para que este pueda ser adecuadamente comprendido en la planificación. Los planes de pruebas proporcionan evidencias de los procedimientos y los criterios de evaluación para evaluar los resultados.		
A tener en cuenta…	**CobiT (Guías de Aseguramiento) Recomienda…**	**ISO 9000 Recomienda…**
Objetivos: Confirmar que la alta gerencia cuenta con: ➢ La definición de sus requisitos para las pruebas de la tecnología que se puede comprar.	➢ Confirme que los principales interesados son considerados en las actividades de prueba de aceptación final. ➢ Averiguar si, y confirme que en las etapas de recepción definitiva, los criterios de éxito son identificados en el plan de pruebas.	

➢ Que se Lleven realmente a cabo los procedimientos de prueba y aceptación para verificar que los recursos adquiridos satisfacen las necesidades de la alta gerencia. **Documentación:** ➢ Requisitos para la presentación de informes de costos y el estado dela gestión de configuración y supervisión de la gestión. ➢ Los registros de los exámenes de configuración u otros informes progreso. ➢ informes de problemas u otros registros de las deficiencias detectadas por el personal de la alta gerencia. ➢ Actas de aceptación de productos. ➢ Prueba de planes para la inspección y aceptación.	➢ Averiguar si, y confirme que la documentación apropiada para su revisión y evaluación existe. ➢ Infórmese a las partes interesadas, que la documentación y presentación de los resultados finales de las pruebas de aceptación están completos y son oportunos.	