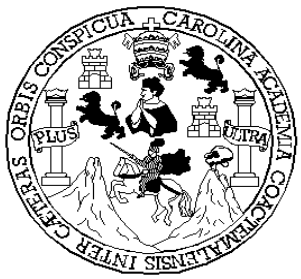
Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Los objetivos de control en la tecnología de información (COBIT) y su aplicación con la auditoría de sistemas

Luis Rafael Gutiérrez Reyes
Asesorado por: Inga. Elizabeth Domínguez Alvarado

Guatemala, julio de 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

Los objetivos de control en la tecnología de información (COBIT) y su aplicación con la auditoría de sistemas

.

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERÍA

POR

LUIS RAFAEL GUTIÉRREZ REYES

ASESORADO POR INGA. ELIZABETH DOMÍNGUEZ ALVARADO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JULIO DE 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahan Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADORA	Inga. Ligia María Pimentel Castañeda
EXAMINADORA	Inga. Elizabeth Domínguez Alvarado
EXAMINADOR	Ing. Luis Alberto Vettorazzi España
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

Los objetivos de control en la tecnología de información (COBIT) y su aplicación con la auditoría de sistemas

Tema que me fuera asignado por la Escuela de Ingeniería en Ciencias y Sistemas con fecha febrero de 2003

LUIS RAFAEL GUTIÉRREZ REYES

AGRADECIMIENTO

1. A la Universidad de San Carlos de Guatemala.

2. A la Facultad de Ingeniería.

3. A la Escuela de Ciencias y Sistemas.

4. Al Colegio Liceo Guatemala.

5. A la Ingeniera Elizabeth Domínguez, por los conocimientos proporcionados durante la asesoría de este trabajo de tesis.

ACTO QUE DEDICO

A DIOS	Todopoderoso, supremo y perfecto. El faro que ilumina cada una de las acciones de mi vida.
A MIS PADRES	Lic. Luis Rafael Gutiérrez Prado. Carlota Reyes de Gutiérrez. Ejemplo a seguir en los pasos de mi vida. Por sus esfuerzos, consejos, sabiduría y apoyo en el logro de mis metas.
A MI ESPOSA	Mariana Anleu de Gutiérrez. El amor eterno e infinito, que siempre me acompaña. Por su incondicional apoyo, su compresión y su fuerza.
A MI HIJA	Marisol Gutiérrez Anleu. Y a mis hijos por venir... La fuente de energía que mueve mi futuro y construye una realidad presente.
A MIS HERMANAS	Astrid Johana Gutiérrez de Erdemenger. Ana Luisa Gutiérrez de Cruz.
A MIS CUÑADOS	Ing. Pablo Erdmenger Pérez. Mario Cruz Wyler.
A MI FAMILIA EN GENERAL	
A MIS COMPAÑEROS DE ESTUDIO	

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Aplicaciones	Se entiende como sistemas de aplicación la suma de procedimientos manuales y programas.
COBIT	"*Control Objectives for Information and related Technology*"; objetivos de control en la tecnología de la información.
COSO	"*Committee of sponsoring organizations*" comisión de estudios de controles internos.
CPA	Instituto americano de contadores públicos.
Datos	Son los elementos de datos en su más amplio sentido, internos, externos, estructurados, no estructurados, etc.
Dominio	Agrupamiento natural de procesos de TI, dentro de una estructura organizacional.
Hardware	Es la parte física de una computadora.
Instalaciones	Recursos para alojar y dar soporte a los sistemas de información.

ISACF	"*Information Systems Audit and Control Foundation*"; fundación del control y auditoría de los sistemas de información.
Objetivo de control	Es una declaración del resultado deseado o propósito a lograr al implementar procedimientos específicos de control, dentro de una actividad de tecnología informática.
Outsourcing	La contratación de servicios terceros para alguna implementación en la tecnología de información.
Personal	Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.
Proceso de TI	Es una serie de actividades o tareas conjuntas con cortes naturales de control.
Recursos de TI	Son todos aquellos datos, aplicaciones, tecnología, instalaciones y personal.
SAC	"*Systems Auditability and Control*"; fundación de investigación del instituto de auditores internos.
SAS 55/78	Consideraciones de la estructura de controles internos, en los informes de los estados financieros del instituto americano de contadores públicos.

Sistema operativo	Es un programa que controla todas las actividades que la computadora realiza. Su función principal consiste en controlar el trabajo que la computadora efectúa.
Sistemas de bases de datos	Es un sistema computarizado, cuyo propósito general es mantener información y hacer que esté disponible cuando se solicite.
Software	Es la parte lógica de una computadora.
Tecnología	La tecnología cubre *hardware*, *software*, sistemas operativos, sistemas de administración de bases de datos, redes, etc.
TI	Tecnología informática.

RESUMEN

Se toman los temas específicos que se aplican sobre una auditoría de sistemas, empezando por una pequeña descripción a nivel general sobre el tema; se definen los antecedentes de la auditoría, las clases que existen, los tipos de controles que se pueden realizar en el sentido informático, y se muestran las utilidades y beneficios que se pueden realizar con una correcta utilización de las herramientas.

Para poder llegar a una explicación más específica, como por ejemplo, los conceptos que se manejan en las diferentes áreas donde se puede aplicar una auditoría a los sistemas de información, así como también los lugares en donde se podría manejar una auditoría de sistemas, es decir, dentro de una base de datos, en el concepto de redes, área física, ofimática, del desarrollo, mantenimiento, técnicas de sistemas, de la calidad, seguridad, de aplicaciones.

Como parte medular de la tesis, se expone y aplica el concepto de una metodología nueva denominada COBIT, que son los objetivos de control en las tecnologías de información; esto ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnologías de Información.

COBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos puramente técnicos y riesgos de negocio. Este habilita el desarrollo de una política clara y de buenas prácticas de control de TI, a través de organizaciones.

Se establece lo que es la auditoría por objetivos de control, su historia y la necesidad de contar con una unión entre el área gerencial y el soporte de sistemas. El

desarrollo de COBIT se puede dividir en diferentes áreas, las cuales se mencionan a continuación:

- Un resumen ejecutivo, que consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT y el marco referencial, el cual está constituido por un entendimiento más detallado de los conceptos clave.

- El marco referencial que describe los 34 objetivos de control de alto nivel e identifica los requerimientos del negocio.

- Los objetivos de control, los cuales contienen declaraciones de los resultados deseados o propósitos que van a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de TI.

- Las directrices de auditoría, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel, para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI.

- Un conjunto de herramientas de implementación, el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

OBJETIVOS

- **General**

  Exponer las principales áreas de la informática, donde se debe aplicar la auditoría, definir su concepto y las formas en la que se puede llevar a cabo, así como ilustrar una nueva metodología en el mercado y su aplicación para el control de tecnología de información por medio de objetivos.

- **Específicos**

  1. Mostrar las técnicas específicas, con las cuales se puede realizar una auditoría de sistemas en cada una de las áreas donde ésta pueda ser aplicable.

  2. Presentar de una forma clara y precisa los conceptos básicos y fundamentales sobre el control interno y auditoría de sistemas.

  3. Definir una metodología aplicativa de la herramienta COBIT, la cual está orientada a ser una herramienta de gobierno de tecnologías de información, que ayude al entendimiento y a la administración de riesgos asociados con tecnologías de información.

  4. Definir, desarrollar y mostrar los pasos de aplicación de la metodología COBIT, en el área de Adquisición e implementación de soluciones de software.

INTRODUCCIÓN

Uno de los elementos importantes, que se deben tomar en consideración, es el desarrollo tecnológico que ha sufrido la humanidad en los últimos treinta años, en los cuales ha cambiado la tecnología de almacenamiento de datos, el transporte de los mismos, la distribución de los sistemas, así como las metodologías para poder desarrollar y adquirir los sistemas de información necesarios para las empresas modernas.

Cada vez más los sistemas informáticos cuentan con una importancia mayor, debido al peso que tiene la correcta información dentro del ámbito empresarial. Es por eso que también los niveles gerenciales necesitan un entendimiento más claro de los procesos y estructuras que utilizan los sistemas, y cada vez más se apoyan e interrelacionan más con los mismos. Esto da como consecuencia que los sistemas sean parte de los activos más valiosos que en la actualidad tenga una empresa.

Con esto la automatización de las actividades empresariales conlleva a que cada vez existan más mecanismos de control en los sistemas de información, sistemas operativos y *hardware*. Con esto nace lo que en la actualidad se conoce como Auditoría de los Sistemas de Información, que se ha convertido en el control del ambiente de controles embebidos en los procesos automatizados y gerenciamiento de los mismos.

La alta dirección gerencial de una organización necesita poder comprender y contar con un conocimiento básico de los riesgos y oportunidades que introduce la incorporación y utilización de la tecnología informática, para lograr una dirección eficaz, segura y confiable.

Para que la alta dirección pueda contar con los elementos de decisión necesaria, se desarrolla COBIT, que es una herramienta desarrollada a partir de los estándares generalmente aplicables y aceptados para la práctica del control de la tecnología Informática.

El tema principal de COBIT es la orientación hacia los negocios. Es un sistema estructurado que se utiliza para el control interno de la tecnología informática, el cual está diseñado para ser empleado por los usuarios y auditores, así como también por los propietarios del proceso del negocio, de una manera sencilla y amigable, con amplio conjunto de preguntas, por medio de las cuales se puede inferir y entender el estado actual de la tecnología de información y los pasos que se van a dar en el mejoramiento de la misma.

El contenido de esta tesis enmarca los conceptos de la auditoría de sistemas de información e invita al lector para que de una manera sencilla pueda aplicar la metodología COBIT, para poder hacer un diagnóstico por medio de los objetivos de control, con la utilización de las herramientas y cuestionarios de diagnóstico que se encuentran en el desarrollo.

Se presentan en su totalidad los objetivos de control en las áreas de planificación y organización, adquisición e implementación, entrega de servicios y soporte y monitoreo.

Por último, se presenta el desarrollo y aplicación de la metodología de COBIT, en el área de Adquisición e Implementación, para lo cual se desarrollan para la misma todas las herramientas necesarias, es decir, los cuestionarios de diagnóstico que resultan del análisis de los objetivos detallados de control y la presentación de matrices de referencia cruzada entre los elementos y los objetivos de control detallado del área estudiada.

1. AUDITORÍA DE SISTEMAS

1.1 Antecedentes

Desde los inicios de la humanidad, las distintas culturas le han dado importancia al tema de la contabilidad, por tanto, a los medios por los cuales se permitiera verificar sus registros, en otras palabras, la auditoría. Sin embargo, no es sino hasta finales de 1,800 cuando la auditoría financiera se extiende por el Reino Unido y Norteamérica, con lo que se logra sentar las bases prácticas que se conocen en la actualidad.

Con la aparición de la primera generación de computadoras en la década de los cincuentas, la informática se convierte en una herramienta muy importante en las labores de la auditoría financiera. Con esto se inicia una "auditoría con el ordenador", ya que no puede considerarse como una verdadera auditoría de los sistemas de información, porque utilizaba al ordenador únicamente como herramienta del auditor financiero.

Alrededor de los años sesentas, los sistemas de información se hacen presentes en las empresas cada vez con mayor frecuencia; a finales de esta década, se empieza a reconocer la necesidad de auditar los sistemas de información. También se funda la Asociación de auditores del proceso electrónico de datos.

Al convertirse los sistemas de información de la organización cada vez más dependientes de los procesos computarizados, surge la necesidad de verificar que los sistemas informáticos funcionan correctamente. A finales de esta década, se descubren algunos casos de fraude cometidos con la ayuda del computador. Surge con esto una nueva especialidad híbrida, que contenga los conceptos de un auditor con los conocimientos técnicos del manejo de sistemas de información.

En la actualidad, uno de los principales activos de las organizaciones, es la información y representa su principal ventaja estratégica, que hace que las empresas inviertan cantidades de tiempo y dinero significativas en la creación de sistemas de información, que les ofrezca una mayor productividad y calidad posible. Ésta es una de las razones, por la cual el tema relacionado con la auditoría de los sistemas de información cobra una mayor relevancia, tanto para su estudio como para su aplicación.

1.2 Auditoría

1.2.1 Concepto

Los orígenes de la palabra auditoría provienen del latín auditorus que significa virtud de oír. De una manera más técnica y conceptual se puede definirla de las siguientes formas:

- Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.
- Es una evaluación de políticas, planes, procesos y procedimientos, controles y práctica de una entidad, que permite detectar desviaciones y presentar las recomendaciones pertinentes.

- Es la aplicación de diversos procedimientos a fin de permitir un juicio técnico.

- Es una revisión objetiva, metódica y completa del logro de los objetivos, sobre la base de los niveles jerárquicos de la empresa.

- Es un examen comprensivo y constructivo de la estructura de una empresa, que abarca los planes, programas, objetivos, métodos y controles.

- Es un proceso que mediante la presentación de alternativas de solución, pretende tomar decisiones correctivas o de mejoramiento de una tarea, actividad, función, procedimiento, proceso o área laboral.

1.2.2 Clases de auditorías

Dentro de la auditoría, se pueden diferenciar distintos enfoques, según el objetivo que se persiga o en función de su importancia. Por consiguiente, la auditoría se puede clasificar de la siguiente forma:

- Financiera: tiene por finalidad presentar la realidad de las cuentas anuales dentro de una organización o empresa. En sí es una revisión de los estados financieros similar a la auditoría externa.
- Informática o sistemas: su finalidad es lograr una operatividad eficiente y, según las normas establecidas dentro de la organización, para los sistemas de aplicación, recursos informáticos y localidades físicas.

- Gestión: su principal objetivo es verificar la eficiencia, eficacia y economicidad de la dirección de una organización empresarial.

- Cumplimiento: su propósito consiste en que todas las operaciones que se realizan dentro de la organización se adecuen conforme a las normas establecidas. El objetivo de ésta de define como la revisión y puesta en práctica de los sistemas, políticas y procedimientos establecidos por la dirección.

1.3 Auditoría de sistemas

1.3.1 Concepto

La auditoría de sistemas se puede definir:

- Como el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

- Como soporte a la auditoría tradicional, financiera, etc., pero añadiendo la función de auditoría de la función de gestión del entorno informático; el cual tiene por objetivo la revisión sistemática del control interno en las actividades involucradas en la administración y control de la operación de las áreas informáticas.
- Como función independiente, enfocada hacia la obtención de la situación actual de un entorno de información e informático, en aspectos de seguridad y riesgo, eficiencia y veracidad e integridad.

1.3.2 Funciones de control interno y auditoría informáticos

El concepto del control interno regularmente no incluía muchas de las actividades operativas claves destinadas a prevenir algunos de los riesgos efectivos y potenciales, lo cual ha provocado cierta cantidad de problemas a las organizaciones.

La mayoría de las organizaciones empresariales han iniciado varias iniciativas en tal sentido, como:

- Reestructuración de los procesos empresariales
- La gestión de calidad total
- El redimensionamiento por reducción y/o por el aumento del tamaño hasta el nivel correcto
- Descentralización
- La contratación externa

Debido al incremento del volumen de recursos y presupuestos que maneja un centro de informática para el manejo de la información perteneciente a los puntos anteriores, aumenta la complejidad de las necesidades del control y auditoría, como medidas organizativas.

1.3.2.1 Control interno informático

La función principal del control interno informático es controlar diariamente que todas las actividades de los sistemas de información sean realizadas, cumpliendo los procedimientos, estándares y normas establecidos.

El propósito de éste es asegurar que las medidas que se pueden obtener de los mecanismos sean correctas y válidas, además de controlar que las actividades que se realizan cumplan con los procedimientos y las normas establecidas para cada una de ellas.

Dentro de éstos se deben definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados del servicio de los sistemas de información.

Las actividades, en las cuales se deben realizar en los diferentes sistemas y entornos informáticos, un control adecuado, son las siguientes:

- El cumplimiento de procedimientos, normas y controles dictados.
- Controles sobre la producción diaria.
- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento de las aplicaciones.
- Controles sobre el *software* de base.
- Controles en las redes de comunicaciones.
- La seguridad informática (usuarios, información clasificada, normas de seguridad, control dual de la seguridad informática).
- Licencias.

1.3.2.2 Auditoría informática

Como se ha definido anteriormente la auditoría de los sistemas de información es el proceso de recoger, agrupar, y evaluar evidencias, para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

De este modo, se puede resumir que el objetivo principal de la auditoría informática es la protección de los activos e integridad de los datos, tomando en cuenta la eficacia y la eficiencia con que se realiza éstas.

Así se pueden llegar a definir las funciones principales y dividirlas en los grupos siguientes:

- Revisar durante y después del diseño, la realización, la implantación y la explotación de las aplicaciones informáticas.

- Revisar y juzgar los controles implantados en los sistemas de información, para verificar su adecuación a las órdenes e instrucciones de la dirección, requisitos legales y fraudes.
- Revisar y evaluar el nivel de eficiencia, utilidad, fiabilidad y seguridad de los equipos e información.

1.3.2.3 Analogía de los anteriores

La evolución que la auditoría de los sistemas de información y los controles internos han tenido ha sido paralela, por lo cual, se pueden encontrar algunas similitudes y diferencias que se enumeran a continuación.

Similitudes :

- Personal Interno.
- Conocimientos especializados en tecnología de información.
- Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos.

Diferencias :

Tabla I. **Diferencias entre control interno y auditoría**

Control interno informático	**Auditoría informática**
Análisis de los controles día a día	Análisis de un momento informático determinado
Información al Departamento de Informática	Información a la dirección general de la organización
Solamente personal interno	Personal interno y/o externo
Alcance de funciones se da solamente sobre el Departamento de Informática	Tiene cobertura sobre todos los componentes de los sistemas de información de la organización

1.3.3 Tipos de controles internos

El control interno es una acción que se realiza manual y/o automáticamente para prevenir, corregir errores o irregularidades que obstaculizan los objetivos de funcionamiento de un sistema de información.

Éstos, cuando se diseñan, desarrollan o se implementan, deben de tener como requisitos mínimos las características de completos, fiables, revisables, adecuados y rentables. Se pueden clasificar de la siguiente manera:

- Controles preventivos

Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, y permiten cierto margen de violaciones.

- Controles detectivos

Son aquellos que no evitan que ocurran las causas del riesgo, sino que los detecta luego de ocurridos. Son los más importantes para el auditor. Sirven para evaluar la eficiencia de los controles preventivos.

- Controles correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, para lo cual es necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

1.3.4 Función de la auditoría informática

1.3.4.1 Definición

Un auditor informático general debe de ser un profesional dedicado al análisis de los sistemas de información e informáticos, que esta especializado en algunas de las múltiples ramas de la auditoría de los sistemas de información, que tiene conocimientos generales de los ámbitos, en los que se mueve y que tenga conocimientos empresariales.

Es una persona que tenga la capacidad para brindar ideas en una situación dada, y además que pueda actuar como consejero dentro de la organización en la que labora.

1.3.4.2 Perfiles profesionales de la función

El auditor de sistemas de información debe de tener un alto grado de calificación técnica y al mismo tiempo estar integrado a las corrientes empresariales actuales, y se debe de contemplar las siguientes características para esbozar un perfil:

- La persona que integre o desarrolle esta función debe de contemplar en su formación una mezcla de conocimientos de auditoría financiera y de informática general, en los aspectos básicos siguientes:

    - Gestión de proyectos.
    - Análisis de riesgos en un entorno informático.
    - Sistema operativo.
    - Telecomunicaciones.
    - Gestión de bases de datos.
    - Redes locales.
    - Seguridad física.

- Operaciones y planificación informática.
- Gestión de seguridad de los sistemas.
- Administración de datos.
- Gestión de problemas y cambios de entornos informáticos.
- Ofimática
- Comercio electrónico
- Encriptación de datos.

- Deberá contar con una especialización en función de la importancia económica, que distintos componentes financieros puedan tener en un entorno empresarial.

- Tener el concepto de calidad total.

1.3.4.3 Funciones por desarrollar

La función de auditoría de sistemas debe de realizar un conjunto de actividades y funciones bastante amplio; los siguientes son algunos ejemplos:

- Verificación del control interno.
- Análisis de la gestión de los sistemas de información, desde un punto de vista de riesgo de seguridad, de gestión y de efectividad de la gestión.
- Análisis de la integridad, fiabilidad y certeza de la información, a través del análisis de las aplicaciones.
- Auditoría del riesgo operativo de los circuitos de información.
- Análisis de la gestión de los riesgos de la información y de la seguridad implícita.
- Verificación del nivel de continuidad de las operaciones.
- Análisis del estado del arte tecnológico de la instalación revisada y de las consecuencias empresariales.

- Diagnóstico sobre el grado de cobertura que dan las aplicaciones a las necesidades estratégicas y operativas de información de la organización.

1.3.5 Organización

Se pueden establecer elementos de control mediante la separación de tareas dentro de las funciones informáticas. Para el tratamiento electrónico de datos, existen dos funciones principales; la primera se refiere al diseño y programación del sistema, mientras que la segunda a la explotación del sistema.

Las áreas principales, en las cuales el auditor informático tendrá como objeto de estudio para poder analizar y asesorar dentro de la organización, son:

- Seguridad
- Control interno operativo
- Eficiencia y eficacia
- Tecnología informática
- Gestión de riesgos

La localización física de las instalaciones, donde se realiza la auditoría de sistemas, puede estar ligada al lugar donde se encuentra el control de auditoría interna, teniendo en cuenta la independencia de objetivos, planes y presupuestos dentro de éstas.

Se debe de contar con accesibilidad total a los sistemas informáticos y de información, sin depender de una misma persona dentro de la empresa ni del departamento de organización, sistemas, financiero y/o administrativo.

El departamento debe de contar con un recurso humano con formación en auditoría y organización, además de contar con personal que cuente con el conocimiento técnico, informático esencial.

El departamento debe contar como mínimo con los responsables y especialistas dentro de cada una de las siguientes áreas:

- Entorno informático y gestión de las bases de datos.
- Comunicaciones y/o redes.
- Gestión de riesgo operativo y aplicaciones.
- Explotación y desarrollo de los sistemas de información.

2. OBJETIVOS DE CONTROL EN TECNOLOGÍA DE INFORMACIÓN – COBIT –

2.1 La auditoria por objetivos de control

Desde la década de 1960, el cambiante y rápido desarrollo de los sistemas de información ha creado la expectativa de una apropiada respuesta de las áreas que se ocupan de gestionar la tecnología informática y sistemas de información.

Muchas organizaciones se están reestructurando a fin de modernizar sus operaciones por medio de departamentos de organización y métodos; simultáneamente se aprovechan los avances en tecnologías de información, a fin de mejorar su posición competitiva. La reingeniería de negocio, el dimensionamiento correcto y el procesamiento distribuido, son todos cambios que afectan la forma en que operan las organizaciones.

Algunas de las causas, por las cuales dentro de las organizaciones modernas la información y los datos, en los que se apoyan, se tornan cada vez más importantes son las siguientes: la alta velocidad con la cual se procesan las transacciones; los sistemas de administración de las bases de datos; las redes de telecomunicaciones globales; el procesamiento distribuido de datos; la comunicación sobre Internet.

Por lo que las estrategias de gerenciamiento, las políticas de seguridad, la segregación de las funciones, el impacto de los fallos, los accesos no autorizados, la revelación de la información, la continuidad del normal procesamiento de los datos, la adecuación de los sistemas de información, y otros aspectos que surgen de la aplicación de innovadoras tecnologías, han pasado a tener un impacto mucho mayor dentro de la organización, que el de hace unos años; de ahí la necesidad de contar con un adecuado marco de control.

Para muchas organizaciones, tanto la información como la tecnología sobre la cual operan, representan actualmente uno de sus activos más valiosos, debido a que han empezado a reconocer los beneficios que estas herramientas tecnológicas pueden proporcionar. Sin embargo, también han comprendido la importancia de conocer y administrar los riesgos asociados con la implementación de las nuevas tecnologías.

2.1.1 Rol de auditoría de sistemas

Los cambios a los cuales están expuestas las organizaciones, debido a la automatización de sus funciones, determina la incorporación de mecanismos de control más potentes en los sistemas de información, así como el enriquecimiento de sus estructuras de control, en los diferentes niveles de *software* y *hardware*. Además, las características estructurales de estos controles están evolucionando al mismo ritmo y de igual manera que estas tecnologías.

En la actualidad, se debe ir hablando más de "Auditoría de Sistemas de Información" que sólo de Auditoría Informática, por la extensión de las áreas que llega a cubrir. En todo caso, la Auditoría de Sistemas de Información se ha convertido en el control del ambiente de controles, embebido en los procesos automatizados y en el gerenciamiento de los mismos.

Esta denominación abarca la necesidad de controlar globalmente a los sistemas de información, es decir, desde su planificación a su implementación, observando también su alineación con las estrategias de la organización, ya que es cierto que en muchos casos es tan necesario o más que la protección de la información, que las inversiones en los sistemas de información y que la tecnología informática estén alineadas con las estrategias de la alta dirección, y escapar al inadecuado enfoque de la tecnología por la tecnología.

También la Auditoría de Sistemas de Información debe contemplar el control del aprovechamiento que se hace de las tecnologías informáticas y si éstas aportan ventajas competitivas, además de la adecuación de la gestión de los recursos tecnológicos y de la seguridad que otorgan.

Debe evaluarse, en la auditoría de sistemas de información, si los modelos de seguridad están en consonancia con las nuevas arquitecturas y las distintas plataformas, porque no se puede auditar con conceptos, técnicas o recomendaciones de hace algunos años atrás.

Así, el enfoque tradicional de la auditoría ha ido evolucionando. Se ha vuelto más participativa, ha priorizado un enfoque preventivo e intentado actuar antes o durante el hecho. La tendencia actual, en el ámbito de la auditoría de sistemas de información, apunta a participar más activamente en todos los proyectos y decisiones relacionados con los sistemas de información y la tecnología informática dentro de la organización.

2.1.2 Marco de control

Las habilidades con las que deben de contar los gerentes, especialistas en sistemas de información y auditores, deben evolucionar con la misma rapidez que lo hace la tecnología y el ambiente de negocios, provocados por los cambios acelerados, y en donde cada uno de ellos desempeñe realmente su rol con efectividad. Deben comprender acabadamente la tecnología de los controles y su naturaleza cambiante; si han de aplicarse criterios razonables y prudentes para evaluar las prácticas de control presentes en las organizaciones.

La alta dirección de cualquier organización necesita poder comprender y contar con un conocimiento básico de los riesgos que introduce la incorporación y utilización de la tecnología informática, para así proveer una dirección eficaz y poner en práctica

todos los mecanismos necesarios, para la puesta en marcha de los controles adecuados. Tiene que decidir cuál es el grado de inversión razonable en seguridad y control, y cómo alcanzar un balance razonable entre el nivel de riesgo y la inversión en los controles.

Planteadas anteriormente muchas de las nuevas exigencias para el incremento de los controles, surge la necesidad de contar con una metodología para organizar las actividades de la auditoría de sistemas de información, la cual contribuya a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos; que sea aplicable a todos los tamaños y tipos de organización y que esté dirigida no sólo a auditores de sistemas, sino también a la administración y a los usuarios; que permita además, determinar el alcance de la tarea de auditoría e identificar los controles mínimos, y que pueda utilizarse como una herramienta de autoevaluación del área de tecnología informática.

2.1.3 Estándares de auditoría

Tanto para los auditores, los gerentes, los contadores, como para las entidades reguladoras en general, en los últimos años se ha incrementado la atención sobre los controles internos. Como resultado se han desarrollado varios documentos para definir, valorizar, reportar y mejorar el control interno y ser utilizados como marco de referencia en las organizaciones. En resumen, éstos son:

- Informe COSO - (*Committee of Sponsoring Organizations*), de la Comisión de Estudios de Controles Internos.
- SAC - (*Systems Auditability and Control*), de la Fundación de Investigación del Instituto de Auditores Internos.
- SAS 55 y SAS 78 - Consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros, del Instituto Americano de Contadores Públicos (CPA)

- COBIT (*Control Objectives for Information and related Technology*), de la Fundación de Auditoría y Control de Sistemas de Información.

Cada uno de éstos ha sido definido para una audiencia en particular: el "COSO" fue diseñado para la Gerencia; el "SAC" para los auditores internos; los SAS 55 y SAS 78 para los auditores externos, y finalmente el "COBIT" enfocado principalmente para los auditores de sistemas de información. Este último es el que se desarrollará más ampliamente.

2.2 Antecedentes

COBIT está basado en los Objetivos de Control existentes de la *Information Systems Audit and Control Foundation* (ISACF); ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de Tecnología Informática. Los objetivos de control resultantes, aplicables y aceptados en forma generalizada, han sido desarrollados para ser aplicados a los sistemas de información de toda la empresa.

Como estándar, se tiene un producto independiente de la plataforma técnica de tecnología informática, que tiende a ser pragmático, relativamente pequeño y que responda a las necesidades del negocio. La provisión de indicadores de performance (normas, reglas, etc.) ha sido identificada como prioridad para las futuras mejoras que se realicen en la estructura.

COBIT resulta gracias a la colaboración y significativas contribuciones de *Unisys*, *Unitech Systems*, *Inc, el MIS Training Institute, Zergo, Ltd y Coopers & Lybrand* para su investigación y publicación. Otras donaciones se recibieron de los Capítulos de ISACA y sus miembros de todo el mundo.

Las organizaciones deben satisfacer con su información, como por todos sus activos, los requerimientos de calidad, información financiera y seguridad. La dirección debe balancear el uso de recursos disponibles incluyendo gente, instalaciones, tecnología, sistemas aplicativos y datos. Para sustentar esta responsabilidad, así como para lograr sus expectativas, la dirección debe establecer un sistema adecuado de control interno. Tal sistema o estructura debe soportar los procesos del negocio y debe ser claro sobre cómo cada actividad individual de control impacta en los recursos y satisface los requerimientos. El control, que incluye políticas, estructuras organizacionales, prácticas y procedimientos es responsabilidad de la dirección.

Un objetivo de control es una declaración del resultado deseado o propósito a lograr al implementar procedimientos específicos de control dentro de una actividad de tecnología informática.

Éste se encuentra diseñado no sólo para ser empleado por los usuarios y los auditores, sino también, y más importante, como un amplio "*checklist*" para los propietarios del proceso del negocio. Uno de los temas principales de COBIT es la orientación hacia los negocios

La estructura es en respuesta a la necesidad de un sistema de control interno en tecnología informática. Esta provee una herramienta para el propietario del proceso del negocio, que facilita el descargo de su responsabilidad. Una de sus premisas dentro de su estructura, con la cual da inicio, es la siguiente:

"Los Recursos de Tecnología Informática necesitan ser administrados por un conjunto de procesos de Tecnología Informática agrupados naturalmente para proveer la información que necesita la empresa para el logro de sus objetivos."

En la Estructura COBIT se destaca el impacto sobre los recursos de Tecnología Informática, junto con los requerimientos del negocio que necesitan ser satisfechos, en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Adicionalmente, la estructura brinda definiciones para los requerimientos del negocio que son destilados de niveles más altos de objetivos según se relacionan con Tecnología Informática.

2.2.1 Desarrollo de producto

Para las buenas prácticas de seguridad y control en Tecnología de Información, COBIT, ha sido desarrollado como un estándar; éste se fundamenta en los objetivos de control existentes de la *Information Systems Audit and Control Foundation* (ISACF). El término buenas prácticas significa el consenso por parte de los expertos.

El proporcionar indicadores de desempeño (normas, reglas, etc.) ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial. El desarrollo de COBIT ha traído como resultado la publicación del marco referencial general y de los objetivos de control detallados.

Como mejoras a los objetivos de control originales, se determinó que éstas debían consistir en:

- El desarrollo de un marco referencial para control en TI como fundamento para los objetivos de control en TI y como una guía para la investigación consistente en auditoría y control de TI.
- Una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho.

- Una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en TI y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.).
- Una revisión crítica y actualización de las guías actuales para desarrollo de auditorías de sistemas de información.

Las fuentes, sin excluir ningún otro estándar aceptado en el campo del control de sistemas de información, son las siguientes:

- Estándares Técnicos de ISO, EDIFACT, etc.
- Códigos de conducta emitidos por el *Council of Europe*, OECD, ISACA, etc.;
- Criterios de Calificación para sistemas y procesos de TI: ITSEC, ISO9000, SPICE, TickIT, etc.;
- Estándares profesionales para control interno y auditoría: reporte COSO, GAO, IFAC, IIA, ISACA, estándares CPA, etc.;
- Prácticas y requerimientos de la Industria de foros industriales (ESF, 14) y plataformas patrocinadas por el gobierno (IBAG, NIST, DTI);
- Nuevos requerimientos específicos de la industria de la banca y manufactura de TI.

2.2.2 Definición y composición del producto

Después de considerar como un elemento crítico para el éxito y la supervivencia de las organizaciones a la administración efectiva de la información y a la Tecnología de Información relacionada, se puede decir que el desarrollo de Cobit ha resultado en la publicación de:

- Un resumen ejecutivo, que consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT y el marco referencial, el cual está constituido por un entendimiento más detallado de los conceptos clave.

- El marco referencial que describe los 34 objetivos de control de alto nivel e identifica los requerimientos del negocio.

- Objetivos de control, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos, a través de los 34 procesos de TI.

- Directrices de auditoría, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel, para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI.

- Un conjunto de herramientas de implementación, el cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

2.3 Necesidad de control en tecnología de información

Uno de los trabajos que actualmente debe desarrollar la administración moderna es el de decidir la inversión razonable en seguridad y control en Tecnología de Información, así como lograr un balance entre los riesgos e inversiones en control de un ambiente de tecnología de información, que es frecuentemente impredecible. A esto se aúnan algunas razones, entre las cuales se pueden mencionar:

- La creciente dependencia en información y en los sistemas que lo proporcionan.
- La creciente vulnerabilidad y un amplio espectro de amenazas.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones, las prácticas de negocio, la creación de oportunidades y la reducción de costos.

Las organizaciones se reestructuran con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en tecnología de sistemas de información para mejorar su posición competitiva. La reingeniería en los negocios, las reestructuraciones, el *outsourcing*, las organizaciones horizontales y el procesamiento distribuido son cambios que impactan la manera en la que operan, tanto los negocios como las entidades gubernamentales. Estos cambios han tenido y continuarán teniendo profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo.

La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en las computadoras y en las redes, tanto los basados en *hardware,* como los basados en *software*. Esto ha conllevado a diferentes modelos de control generales de negocios, como el COSO, además existe un número importante de modelos de control más orientados al nivel de tecnología de información.

Estos modelos con orientación específica no proporcionan un modelo de control completo y utilizable sobre tecnología de información como soporte para los procesos de negocio. El propósito de COBIT es cubrir este vacío proporcionando una base que esté estrechamente ligada a los objetivos de negocio, al mismo tiempo que se enfoca a la tecnología de información.

El objetivo principal del proyecto COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de tecnología de información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es desarrollar estos objetivos de control, principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa.

2.3.1 Definiciones y usuarios

Para propósitos informativos, se definirán los términos control y objetivo en control en tecnología de información de la siguiente manera:

- Control: las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados, y que los eventos no deseables sean prevenidos o detectados y corregidos.
- Objetivo de control en tecnología de información: una definición del resultado o propósito que se desea alcanzar cuando se implementan procedimientos de control en una actividad de TI particular.

COBIT está diseñado para ser utilizado por tres tipos o conjuntos de usuarios distintos:

- Administración: es para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

- Usuarios: para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

- Auditores de sistemas de información: es para dar soporte a las opiniones mostradas a la administración sobre los controles internos.

Además de responder a las necesidades de la audiencia inmediata de la Alta Gerencia, a los auditores y a los profesionales dedicados al control y seguridad, COBIT puede ser utilizado dentro de las empresas por el propietario de procesos de negocio en su responsabilidad de control, sobre los aspectos de información del proceso, y por todos aquellos responsables de TI en la empresa.

3. DESARROLLO DEL MODELO Y OBJETIVOS DE CONTROL

3.1 Modelos de control

Existen dos clases distintas de modelos de control disponibles actualmente; aquellos de la clase del "modelo de control de negocios" (por ejemplo COSO) y los "modelos más enfocados a TI" (por ejemplo, DTI). COBIT se posiciona como una herramienta más completa para la administración y para operar a un nivel superior que los estándares de tecnología para la administración de sistemas de información.

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en tecnología de información se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la tecnología de información, que deben ser administrados por procesos de TI.

3.1.1 Requerimientos de negocio para la información

Es necesario concordar ciertos criterios, para satisfacer los objetivos de negocio y la información; COBIT hace referencia a ellos como los requerimientos de negocio para la información, y combina los principios contenidos en los modelos existentes y conocidos:

- Requerimientos de calidad
    - Calidad
    - Costo
    - Entrega (servicio)

La calidad ha sido considerada principalmente por su aspecto negativo, es decir, no fallas, confiable etc. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega (de servicio) de la calidad se traslapa con el aspecto de disponibilidad, correspondiente a los requerimientos de seguridad y también, en alguna medida, con la efectividad y la eficiencia.

- Requerimientos fiduciarios
    - Efectividad y eficiencia de operaciones
    - Confiabilidad de la información
    - Cumplimiento de leyes y regulaciones

Para los requerimientos fiduciarios en COBIT, se utilizaron las definiciones de COSO, para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, la confiabilidad de información fue ampliada para incluir toda la información de la siguiente manera:

- Requerimientos de seguridad
    - Confidencialidad
    - Integridad
    - Disponibilidad

Respecto a los aspectos de seguridad, fue descubierto que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

3.1.1.1 Definiciones de trabajo

A partir de los anteriores requerimientos de negocios para la información y tomando en cuenta cada unas de ellas, se pueden extraer siete categorías distintas, ciertamente superpuestas a las cuales, se llamarán definiciones de trabajo de COBIT, las cuales se listan a continuación:

- Efectividad: se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

- Eficiencia: se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

- Confidencialidad: se refiere a la protección de información sensible contra divulgación no autorizada.

- Integridad: se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

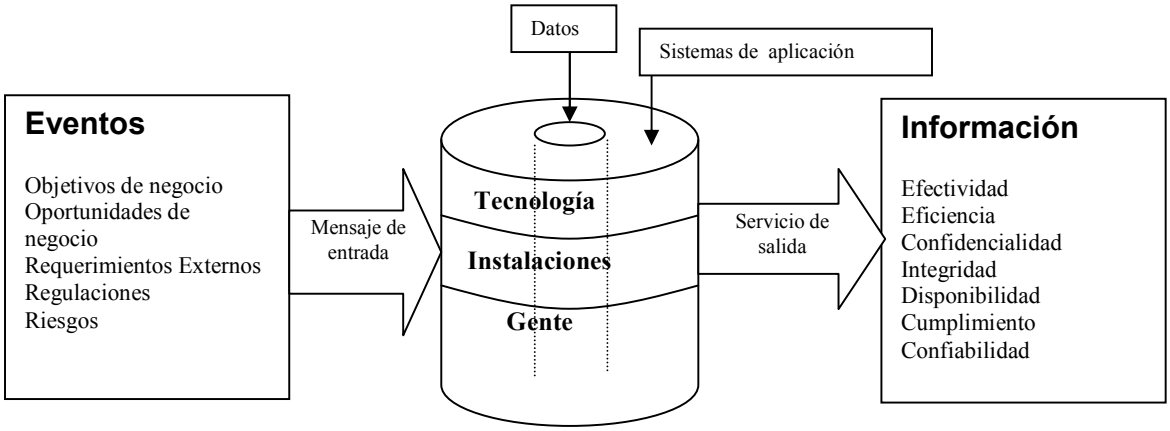
- Disponibilidad: se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto.

- Confiabilidad de la Información: se refiere a la provisión de información apropiada para la administración, con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

3.1.2 Recursos de TI

Una forma de ver la relación de los recursos de tecnología de información, respecto a la entrega de servicios es que la información que los procesos de negocios necesitan es proporcionada a través del empleo de recursos de Tecnología de Información. Con el fin de asegurar que los requerimientos de negocios para la información son satisfechos, deben de definirse, implementarse y monitorearse medidas de control adecuadas para éstos recursos, el cual se ilustra en la siguiente gráfica (Figura 1):

Figura 1. **Recursos de TI**



Los recursos de tecnología de información se pueden explicar o definir de la siguiente manera:

- Datos: los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

- Aplicaciones: se entiende como sistemas de aplicación la suma de procedimientos manuales y programas.

- Tecnología: la tecnología cubre *hardware, software*, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

- Instalaciones: recursos para alojar y dar soporte a los sistemas de información.

- Personal: habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

3.1.3 Procesos de TI

El marco referencial consta de objetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI, al considerar la administración de sus recursos. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas.

La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI. En resumen, los procesos de tecnología de información se pueden agrupar en tres grandes categorías:

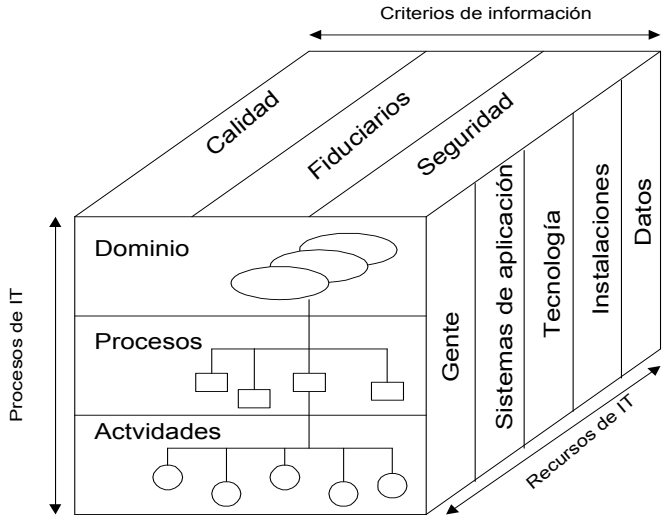
- Dominios
- Procesos
- Actividades

Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos de vista estratégicos:

- Recursos de tecnología de información
- Requerimientos de negocio para la información
- Procesos de tecnología de información

Éstos son diagramados para examinarlos de manera visual en el siguiente cubo de Información:

Figura 2. **Procesos de TI**



3.1.4 Definiciones para dominios

Con lo anterior como marco de referencia, los dominios son identificados empleando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización.

Cuatro grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo. Las definiciones para los dominios mencionados son las siguientes:

- Planeación y organización*:* este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma, en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.

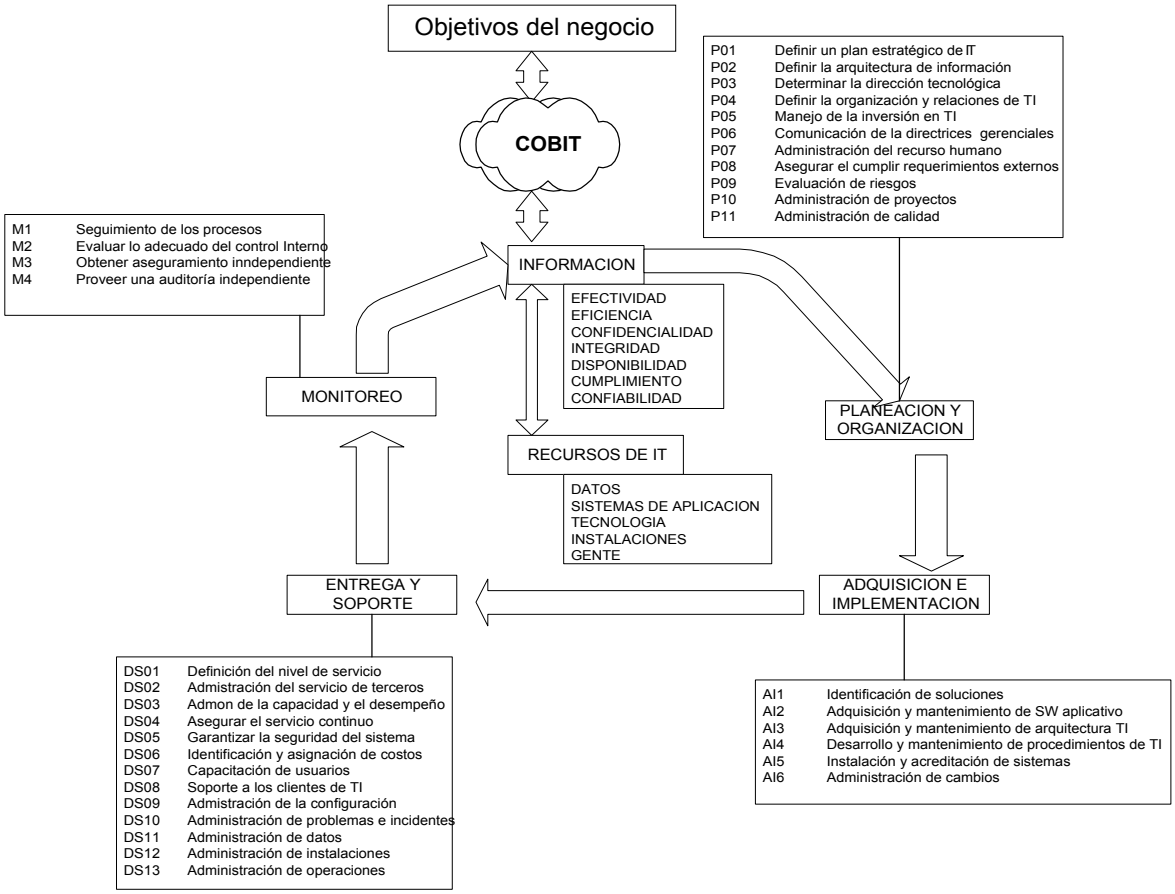
- Adquisición e implementación: para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio.

- Entrega y soporte: en este dominio, se hace referencia a la entrega de los servicios requeridos, que comprende desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- Monitoreo: todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia, en cuanto a los requerimientos de control.

En resumen, los recursos de tecnología de información necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos. El cual se ilustra en el siguiente diagrama (figura 3) :

Figura 3. **Estructura y objetivos de Cobit**



3.1.5 Clasificación de marco de referencia del producto

Se lleva a cabo una clasificación, dentro del marco referencial COBIT, basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente.

- Primario es el grado al cual el objetivo de control definido, en que impacta directamente el requerimiento de información de interés.

- Secundario es el grado, al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

- Blanco (vacío) podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Similarmente, todas las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el marco referencial de COBIT indica específicamente la aplicabilidad de los recursos de TI, que son administrados en forma específica por el proceso bajo consideración.

3.2 Desarrollo de objetivos de control

Los objetivos de control se distribuirán como se muestra en la siguiente tabla:

Tabla II. **Objetivos de control**

			Criterios de información								**Recursos de TI**				
Dominio		**Proceso**	**efectividad**	**eficiencia**	**confidencialidad**	**integridad**	**disponibilidad**	**cumplimiento**	**confiabilidad**		**recursos**	**sistemas de aplicación**	**tecnología**	**instalaciones**	**datos**
Planeación y organización	PO1	Definir un plan estratégico de TI	P	S							¤	¤	¤	¤	¤
	PO2	Definir la arquitectura de información	P	S	S	S						¤			¤
	PO3	Determinar la dirección tecnológica	P	S									¤	¤	
	PO4	Definir la organización y relaciones de TI	P	S							¤				
	PO5	Manejo de la inversión en TI	P	P					S		¤	¤	¤	¤	
	PO6	Comunicación de la directrices gerenciales	P					S			¤				
	PO7	Administración del recurso humano	P	P							¤				
	PO8	Asegurar el cumplir requerimientos externos	P					P	S		¤	¤			¤
	PO9	Evaluación de riesgos	S	S	P	P	P	S	S		¤	¤	¤	¤	¤
	PO10	Administración de proyectos	P	P							¤	¤	¤	¤	
	PO1	Administración de	P	P		P			S		¤	¤			

	1	calidad													
Adquisición e implementación	AI1	Identificación de soluciones	P	S								¤	¤	¤	
	AI2	Adquisición y manten. De SW aplicativo	P	P		S		S	S			¤			
	AI3	Adquisición y manten. de arquitectura TI	P	P		S							¤		
	AI4	Desarrollo y mantenimiento de procedimientos de TI	P	P		S		S	S		¤	¤	¤	¤	
	AI5	Instalación y acreditación de sistemas	P			S	S				¤	¤	¤	¤	¤
	AI6	Administración de cambios	P	P		P	P		S		¤	¤	¤	¤	¤
Entrega de servicios y soporte	DS01	Definición del nivel de servicio	P	P	S	S	S	S	S		¤	¤	¤	¤	¤
	DS02	Administración del servicio de terceros	P	P	S	S	S	S	S		¤	¤	¤	¤	¤
	DS03	Admón. de la capacidad y el desempeño	P	P			S					¤	¤	¤	
	DS04	Asegurar el servicio continuo	P	S			P				¤	¤	¤	¤	¤
	DS05	Garantizar la seguridad del sistema			P	P	S	S	S		¤	¤	¤	¤	¤
	DS06	Identificación y asignación de costos		P					P		¤	¤	¤	¤	¤

	DS07	Capacitación de usuarios	P	S							¤					
	DS08	Soporte a los clientes de TI	P								¤	¤				
	DS09	Administración de la configuración	P				S		S			¤	¤	¤		
	DS10	admón.. de problemas e incidentes	P	P			S				¤	¤	¤	¤	¤	
	DS11	Administración de datos				P			P						¤	
	DS12	Administración de instalaciones				P	P							¤		
	DS13	Administración de operaciones	P	P		S	S				¤	¤		¤	¤	
Monitoreo	M1	Seguimiento de los procesos	P	S	S	S	S	S	S		¤	¤	¤	¤	¤	
	M2	Evaluar lo adecuado del control interno	P	P	S	S	S	S	S		¤	¤	¤	¤	¤	
	M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S		¤	¤	¤	¤	¤	
	M4	Proveer una auditoría independiente	P	P	S	S	S	S	S		¤	¤	¤	¤	¤	

3.2.1 Objetivos generales de planificación y organización

3.2.1.1 Definición de un plan estratégico de tecnología de información

Es el que satisface los requerimientos de negocio, que consiste en lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, así como para asegurar sus logros futuros.

Se hace posible a través de un proceso de planeación estratégica emprendido en intervalos regulares, que da lugar a planes a largo plazo. Los planes a largo plazo deberán ser traducidos periódicamente en planes operacionales y establecer metas claras y concretas a corto plazo.

Y toma en consideración:

- Definición de objetivos de negocio y necesidades de TI
- Inventario de soluciones tecnológicas e infraestructura actual
- Servicios de vigilancia tecnológica
- Cambios organizacionales
- Estudios de factibilidad oportunos
- Evaluación de sistemas existentes

Tabla III. **Criterios y recursos en el plan estratégico de TI**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	Integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	S							¤	¤	¤	¤	¤

Objetivos de control detallados

a) Tecnología de información como parte del plan de la organización a corto y largo plazo.

La alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo, que satisfagan la misión y las metas de la organización. A este respecto, la alta gerencia deberá asegurar que los problemas de tecnología de información, así como las oportunidades, sean evaluados adecuadamente y reflejados en los planes a largo y corto plazo de la organización.

b) Plan a largo plazo de tecnología de información

La gerencia de la función de servicios de información será responsable de desarrollar regularmente planes a largo plazo de tecnología de información, que apoyen el logro de la misión y las metas generales de la organización. De la misma manera, la Gerencia deberá implementar un proceso de planeación a largo plazo, adoptar un enfoque estructurado y determinar la estructura para el plan.

c) Plan a largo plazo de tecnología de información - enfoque y estructura

La gerencia de la función de servicios de información deberá establecer y aplicar un enfoque estructurado al proceso de planeación a largo plazo. Esto deberá traer como resultado un plan de alta calidad, que cubra las preguntas básicas de qué, quién y cuándo. Los aspectos que necesitan ser tomados en cuenta y ser cubiertos adecuadamente durante el proceso de planeación son el modelo de organización y sus cambios, la distribución geográfica, la evolución tecnológica, los costos, los requerimientos legales y regulatorios, requerimientos de terceras partes o del mercado, el horizonte de planeación, reingeniería de procesos del negocio, la asignación de personal, la designación de fuentes internas o externas, etc.

El plan mismo deberá hacer referencia a otros planes, como el plan de calidad de la organización y el plan de manejo de riesgos de información.

d) Cambios al plan a largo plazo de tecnología de información

La gerencia de la función de servicios de información deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información, con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la tecnología de información.

e) Planeación a corto plazo para la función de servicios de información

La gerencia de la función de servicios de información deberá asegurar que el plan a largo plazo de tecnología de información sea traducido regularmente en planes a corto plazo de tecnología de información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de tecnología de información, con una base consistente con el plan a largo plazo de tecnología de información.

Los planes a corto plazo deberán ser reevaluados y modificados periódicamente, según se considere necesario, que respondan a las condiciones de cambios en el negocio y en la tecnología de información. La realización oportuna de estudios de factibilidad deberá asegurar que la ejecución de los planes a corto plazo sea iniciada adecuadamente.

f) Evaluación de sistemas existentes

En forma previa al desarrollo o modificación del plan estratégico de TI, la gerencia de servicios de información debe evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de

determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

3.2.1.2 Definición de la arquitectura de información

Monitoreo

El objetivo que satisface los requerimientos de negocio de organizar de la mejor manera los sistemas de información, se hace posible a través de la creación y mantenimiento de un modelo de información de negocios, asegurando que se definan sistemas apropiados para optimizar la utilización de esta información.

Y toma en consideración:

- La documentación
- El diccionario de datos
- Las reglas de sintaxis de datos
- La propiedad de la información y clasificación de severidad

Tabla IV. **Criterios y recursos en la arquitectura de la información**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Personas	aplicación	Tecnología	Instalaciones	Datos
P	S	S	S						¤			¤

Objetivos de control detallados

a) Modelo de la arquitectura de información

La información deberá conservar consistencia con las necesidades y deberá ser identificada, capturada y comunicada en una forma y dentro de períodos de tiempo, que permitan a los responsables llevar a cabo sus tareas eficiente y oportunamente. Asimismo, la función de sistemas de información deberá crear y actualizar regularmente un modelo de arquitectura de información, abarcando el modelo de datos corporativo y los sistemas de información asociados. El modelo de arquitectura de información deberá conservar consistencia con el plan a largo plazo de tecnología de información.

b) Diccionario de datos y reglas de sintaxis de datos de la corporación

La función de servicios de información deberá asegurar la creación y la continua actualización de un diccionario de datos corporativo, que incorpore las reglas de sintaxis de datos de la organización.

c) Esquema de clasificación de datos

Deberá establecerse un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información (por ejemplo, categorías de seguridad), así como a la asignación de propiedad. Las reglas de acceso para las clases deberán definirse apropiadamente.

d) Niveles de seguridad

La gerencia deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de control apropiado (mínimo) para cada una de las clasificaciones.

3.2.1.3 Determinación de la dirección tecnológica

Es el objetivo que satisface los requerimientos de negocio de aprovechar la tecnología disponible o tecnología emergente.

Se hace posible a través de la creación y mantenimiento de un plan de infraestructura tecnológica.

Y toma en consideración:

- La capacidad de adecuación y evolución de la infraestructura actual
- El monitoreo de desarrollos tecnológicos
- Las contingencias
- Los planes de adquisición

Tabla V. **Criterios y recursos en la dirección tecnológica**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	S									¤	¤	

Objetivos de control detallados

a) Planeación de la infraestructura tecnológica

La función de servicios de información deberá crear y actualizar regularmente un plan de infraestructura tecnológica, que concuerde con los planes a largo y corto plazo de tecnología de información. Dicho plan deberá abarcar aspectos como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

b) Monitoreo de tendencias y regulaciones futuras

La función de servicios de información deberá asegurar el continuo monitoreo de tendencias futuras y condiciones regulatorias, de tal manera que estos factores puedan ser tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

c) Contingencias en la infraestructura tecnológica

El plan de infraestructura tecnológica deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura).

d) Planes de adquisición de *hardware* y *software*

La gerencia de la función de servicios de información deberá asegurar que los planes de adquisición de *hardware* y *software* sean establecidos y que reflejen las necesidades identificadas en el plan de infraestructura tecnológica.

e) Estándares de tecnología

Tomando como base el plan de infraestructura tecnológica, la gerencia deberá definir normas de tecnología con la finalidad de fomentar la estandarización.

3.2.1.4 Definición de la organización y de las relaciones de TI

P

Objetivo que satisface los requerimientos de negocio de prestación de servicios de TI, se hace posible a través de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas.

Y toma en consideración:

- El comité de dirección

- La responsabilidades en el ámbito de alta gerencia o del consejo
- La propiedad, custodia
- La supervisión
- La segregación de funciones
- Los roles y responsabilidades
- La descripción de puestos
- Los niveles de asignación de personal
- El personal clave

Tabla VI. **Criterios y recursos en la definición de la organización**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		recursos				
P	S							¤				

Objetivos de control detallados

a) Comité de planeación o dirección de la función de servicios de información

La alta gerencia de la organización deberá designar un comité de planeación o dirección, para vigilar la función de servicios de información y sus actividades. Entre los miembros del comité deberán encontrarse

representantes de la alta gerencia, de la gerencia usuaria y de la función de servicios de información. El comité deberá reunirse regularmente y reportar a la alta gerencia.

b) Ubicación de los servicios de información en la organización

Al ubicar la función de servicios de información en la estructura organizacional general, la alta gerencia deberá asegurar la existencia de autoridad, actitud crítica e independencia por parte del departamento usuario, con un grado tal que sea posible garantizar soluciones de tecnología de información efectivas y progreso suficiente al implementarlas, así como establecer una relación de sociedad con la alta gerencia, para incrementar la capacidad de previsión, la comprensión y las habilidades para identificar y resolver problemas de tecnología de información.

c) Revisión de logros organizacionales

Deberá establecerse un marco de referencia, con el propósito de revisar que la estructura organizacional cumpla continuamente con los objetivos y se adapte a las cambiantes circunstancias.

d) Funciones y responsabilidades

La gerencia deberá asegurar que todo el personal en la organización conozca sus funciones y responsabilidades, en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad respecto a la seguridad y al control interno. Consecuentemente, deberán organizarse y emprenderse campañas regulares para aumentar la conciencia y la disciplina.

e) Responsabilidad del aseguramiento de la calidad

La gerencia deberá asignar la responsabilidad de la ejecución de la función de aseguramiento de calidad a miembros del personal de la función de servicios de información, y asegurar que existan sistemas de aseguramiento de calidad apropiados, controles y experiencia en comunicación dentro del grupo de aseguramiento de calidad de la función de servicios de información. La ubicación de la función dentro del área de servicios de información, las responsabilidades y el tamaño del grupo de aseguramiento de calidad, deberán satisfacer los requerimientos de la empresa.

f) Responsabilidad de la seguridad lógica y física

La gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un gerente de seguridad de la información, quien se reportará a la alta gerencia. Como mínimo, la responsabilidad de la gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización.

En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos, con el fin de resolver los problemas de seguridad relacionados con ellos.

g) Propiedad y custodia

La gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

h) Propiedad de datos y sistemas

La gerencia deberá asegurar que todos los activos de información (sistemas y datos) cuenten con un propietario asignado que tome decisiones sobre la clasificación y los derechos de acceso. Los propietarios del sistema normalmente delegarán la custodia diaria al grupo de liberación operación de sistemas y las responsabilidades de seguridad a un administrador de la seguridad. Los propietarios, sin embargo, permanecerán como responsables del mantenimiento de medidas de seguridad apropiadas.

i) Supervisión

La alta gerencia deberá implementar prácticas de supervisión adecuadas en la organización de servicios de información, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente, para evaluar si todo el personal cuenta con suficiente autoridad y recursos para llevar a cabo sus tareas y responsabilidades, y para revisar de manera general los indicadores clave de desempeño.

j) Segregación de funciones

La alta gerencia deberá implementar una división de funciones y responsabilidades, que excluya la posibilidad de que un solo individuo resuelva un proceso crítico. La gerencia deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones:

- Uso de sistemas de información
- Entrada de datos
- Operación de cómputo
- Administración de redes
- Administración de sistemas
- Desarrollo y mantenimiento de sistemas
- Administración de cambios
- Administración de seguridad
- Auditoría de seguridad

k) Asignación de personal para tecnología de información

Las evaluaciones de los requerimientos de asignación de personal deberán llevarse a cabo regularmente, para asegurar que la función de servicios de información cuente con un número suficiente de personal competente de tecnología de información.

Los requerimientos de asignación de personal deberán ser evaluados, por lo menos anualmente o al presentarse cambios mayores en el negocio, en el ambiente operacional o de tecnología de información. Deberá actuarse oportunamente tomando como base los resultados de las evaluaciones, para asegurar una asignación de personal adecuada en el presente y en el futuro.

l) Descripción de puestos para el personal de la función de servicios de información

La gerencia deberá asegurar que las descripciones de los puestos para el personal de la función de servicios de información sean establecidos y actualizados regularmente. Estas descripciones de puestos deberán delinear claramente tanto la responsabilidad como la autoridad; incluir las

definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

m) Personal clave de TI

La gerencia deberá definir e identificar al personal clave de tecnología de información.

n) Procedimientos para personal por contrato

La gerencia deberá definir e implementar procedimientos relevantes para controlar las actividades de consultores y demás personal externo contratado por la función de servicios de información, para asegurar la protección de los activos de información de la organización.

o) Relaciones

La gerencia de la función de servicios de información deberá llevar a cabo las acciones necesarias para establecer y mantener una coordinación, una comunicación y un enlace óptimos entre la función de servicios de información y demás elementos interesados dentro y fuera de la función de servicios de información (usuarios, proveedores, oficiales de seguridad, Gerentes).

3.2.1.5 Manejo de la inversión

El objetivo principal que satisface los requerimientos de negocio para asegurar el financiamiento y el control de desembolsos de recursos financieros, se hace posible a través de presupuestos periódicos sobre inversiones y operación establecidos y aprobados por el negocio.

Y toma en consideración:

- Alternativas de financiamiento
- Control del gasto real
- Justificación de costos
- Justificación del beneficio

Tabla VII. **Criterios y recursos en el manejo de la inversión**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	Datos
P	P					S		¤	¤	¤	¤	

Objetivos de control detallados

a) Presupuesto operativo anual para la función de servicios de información

La alta gerencia deberá implementar un proceso de definición de presupuestos, para asegurar que un presupuesto operativo anual para la función de servicios de información sea establecido y aprobado en línea con los planes a largo y corto plazo de la organización, así como con los planes a largo y corto plazo de tecnología de información. Deberán investigarse alternativas de financiamiento.

b) Monitoreo de costo – beneficios

La gerencia deberá establecer un proceso de monitoreo de costos, que compare los costos reales contra los presupuestados. Aun más, los posibles beneficios derivados de la actividad de tecnología de información deberán ser identificados y reportados. En cuanto al monitoreo de costos, la fuente de las cifras reales deberá tomar como base el sistema de contabilidad de la organización, el cual deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información. En lo que corresponde a monitoreo de beneficios, se deberán definir indicadores de medición de desempeño de alto nivel y ser reportados y revisados regularmente para asegurar su adecuación.

c) Justificación de costo – beneficio

Deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos, y se encuentre en línea con la industria. Los beneficios derivados de las actividades de tecnología de información deberán ser analizados en forma similar.

3.2.1.6 Comunicación de la dirección y aspiraciones de la gerencia

El objetivo que satisface los requerimientos de negocio de asegurar el conocimiento y comprensión del usuario sobre dichas aspiraciones, se hace posible a través de políticas establecidas y transmitidas a la comunidad de usuarios; además, se necesitan estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables.

Y toma en consideración:

- El Código de ética / conducta
- Las Directrices tecnológicas
- El Cumplimiento
- El Compromiso con la calidad
- Las Políticas de seguridad
- Las Políticas de control interno

Tabla VIII. **Criterios y recursos para la comunicación entre la dirección y la gerencia**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	confidencialidad	integridad	disponibilidad	Cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P					S			¤				

Objetivos de control detallados

a) Ambiente positivo de control de la información

La gerencia deberá crear un marco de referencia y un programa de previsión que fomente un ambiente de control positivo, a través de toda la organización al aplicar elementos como: integridad, valores éticos, competencia del empleado, filosofía y estilo operativo de la gerencia, responsabilidad, atención y dirección proporcionadas por el Consejo Directivo. Deberá ponerse especial atención a los aspectos relacionados con tecnología de información.

b) Responsabilidad de la gerencia en cuanto a políticas

La gerencia deberá asumir la responsabilidad completa de la formulación, el desarrollo, la documentación, la promulgación y el control de políticas que cubran metas y directrices generales. Deberán llevarse a cabo revisiones regulares de las políticas para asegurar su conveniencia. La complejidad de las políticas y los procedimientos escritos deberán estar siempre en proporción con el tamaño de la organización y el estilo gerencial.

c) Comunicación de las políticas de la organización

La gerencia deberá asegurar que las políticas organizacionales sean comunicadas y comprendidas por todos los niveles de la organización.

d) Recursos para la implementación de políticas

Posterior a la comunicación, la gerencia deberá destinar recursos para la implementación de sus políticas. La gerencia deberá también monitorear la duración de la implementación de sus políticas.

e) Mantenimiento de políticas

Las políticas deberán ser ajustadas regularmente para adecuarse a las condiciones cambiantes. Las políticas deberán ser reevaluadas, por lo menos anualmente o en el momento de presentarse cambios significativos en el ambiente operacional o del negocio, para evaluar que sean convenientes y apropiadas, y deberán ser modificadas en caso necesario. La gerencia deberá proporcionar un marco de referencia y un proceso para las revisiones periódicas y la aprobación de estándares, políticas, directrices y procedimientos.

f) Cumplimiento de políticas, procedimientos y estándares

La Gerencia deberá asegurar que se establezcan procedimientos apropiados, para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por la alta gerencia, y promoverse a través del ejemplo.

g) Compromiso con la calidad

La gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, así como políticas y objetivos que sean consistentes con la filosofía y las políticas de la corporación a este respecto. La filosofía de calidad, las políticas y los objetivos deberán ser comprendidos, implementados y mantenidos a todos los niveles de la función de servicios de información.

h) Política sobre el marco de referencia para la seguridad y el control interno

La gerencia deberá asumir la responsabilidad total del desarrollo y mantenimiento de una política sobre el marco de referencia, que establezca el enfoque general de la organización en cuanto a seguridad y control interno. La política deberá cumplir con los objetivos generales del negocio y estar dirigida a la minimización de riesgos, a través de medidas preventivas, identificación oportuna de irregularidades, limitación de pérdidas y recuperación oportuna. Estas medidas deberán basarse en análisis costo-beneficio y deberá priorizarse.

Además, la alta gerencia deberá asegurar que esta política de seguridad de alto nivel y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento con las políticas de seguridad y control interno.

i) Derechos de propiedad intelectual

La gerencia deberá proveer e implementar una política por escrito sobre derechos de propiedad intelectual, que cubra el desarrollo de software, tanto interno como contratado a externos.

j) Políticas para situaciones específicas

Deberán ponerse en práctica medidas que aseguren el establecimiento de políticas para situaciones específicas, con el fin de documentar las decisiones gerenciales respecto al tratamiento de actividades, aplicaciones, sistemas o tecnologías particulares.

3.2.1.7 Administración de RR HH

El objetivo principal que satisface los requerimientos de negocio de maximizar las contribuciones del personal a los procesos de TI, se hace posible a través de técnicas sólidas para administración de personal.

Toma en consideración:

- El reclutamiento y promoción
- Los requerimientos de calificaciones
- La capacitación
- El desarrollo de conciencia
- El entrenamiento cruzado
- Los procedimientos de acreditación
- La evaluación objetiva y medible del desempeño

Tabla IX. **Criterios y recursos para la administración de RRHH**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P							¤				

Objetivos de control detallados

a) Reclutamiento y promoción de personal

La gerencia deberá implementar y evaluar regularmente los procesos necesarios para asegurar que las prácticas de reclutamiento y promoción de personal tengan como base criterios objetivos y consideren factores como la educación, la experiencia y la responsabilidad.

Estos procesos deberán estar en línea con las políticas y procedimientos generales de la organización a este respecto.

b) Personal calificado

La gerencia de la función de servicios de información deberá verificar regularmente que el personal que lleva a cabo tareas específicas esté calificado, tomando como base una educación, entrenamiento y/o experiencia

apropiados, según se requiera. La gerencia deberá alentar al personal para que participe como miembro, en organizaciones profesionales.

c) Entrenamiento de personal

La gerencia deberá asegurar que los empleados reciban orientación al ser contratados, así como entrenamiento y capacitación constantes con la finalidad de conservar los conocimientos, habilidades, destrezas y conciencia de seguridad al nivel requerido, para la ejecución efectiva de sus tareas.

Los programas de educación y entrenamiento dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal deberán ser revisados regularmente.

d) Entrenamiento cruzado o respaldo de personal

La gerencia deberá proporcionar un entrenamiento "cruzado" o contar con suficiente personal de respaldo, con la finalidad de solucionar posibles ausencias.

El personal encargado de puestos delicados deberá tomar vacaciones ininterrumpidas con una duración suficiente, como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

e) Procedimientos de acreditación de personal

La gerencia de la función de servicios de información deberá asegurar que su personal se sujete a una revisión o acreditación de seguridad antes de

ser contratado, transferido o promovido, que depende de lo delicado o sensible del puesto.

Un empleado que no haya pasado por este procedimiento de revisión o acreditación al ser contratado por primera vez, no deberá ser colocado en un puesto delicado, hasta que éste haya obtenido la acreditación de seguridad.

f) Evaluación de desempeño de los empleados

La gerencia deberá implementar un proceso de evaluación de desempeño de los empleados y asegurar que dicha evaluación sea llevada a cabo regularmente, según los estándares establecidos y las responsabilidades específicas del puesto.

Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

g) Cambios de puesto y despidos

La gerencia deberá asegurar que se tomen acciones oportunas y apropiadas, respecto a cambios de puesto y despidos, de tal manera que los controles internos y la seguridad no se vean perjudicados por estos eventos.

3.2.1.8 Cumplimiento de requerimientos externos

El objetivo que satisface los requerimientos de negocio de cumplir con obligaciones legales, regulatorias y contractuales, se hace posible a través de la identificación y análisis de los requerimientos externos en cuanto a su impacto en TI; para esto se llevan a cabo las medidas apropiadas para cumplir con ellos.

Y toma en consideración:

- Las leyes, regulaciones, contratos
- El monitoreo de evoluciones legales y regulatorios
- Las revisiones regulares en cuanto a cambios
- La búsqueda de asistencia legal y modificaciones
- La seguridad y ergonomía
- La privacidad
- La propiedad intelectual
- El flujo de datos

Tabla X. **Criterios y recursos para el cumplimiento de requerimientos**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	Disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P					P	S		¤	¤			¤

Objetivos de control detallados

a) Revisión de requerimientos externos

La organización deberá establecer y mantener procedimientos para la revisión de requerimientos externos y para la coordinación de estas actividades. La investigación continua deberá determinar los requerimientos externos aplicables en la organización. Deberán revisarse los requerimientos legales, gubernamentales o cualquier otro requerimiento externo relacionado con las prácticas y controles de tecnología de información. La gerencia deberá también evaluar el impacto de cualquier relación externa en las necesidades generales de información de la organización, incluyendo la determinación del grado al cual las estrategias de la función de servicios de información deben soportar o cumplir con los requerimientos de terceros.

b) Prácticas y procedimientos para el cumplimiento de requerimientos externos

Las prácticas organizacionales deberán asegurar que se lleven a cabo oportunamente las acciones correctivas apropiadas para garantizar el cumplimiento de los requerimientos externos. Además, deberán establecerse y mantenerse los procedimientos adecuados que aseguren el cumplimiento continuo. A este respecto, la gerencia deberá solicitar apoyo legal en caso necesario.

c) Cumplimiento de seguridad y ergonomía

La gerencia deberá asegurar el cumplimiento de los estándares ergonómicos y de seguridad en el ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

d) Privacidad, propiedad intelectual y flujo de datos

La gerencia deberá asegurar el cumplimiento de las regulaciones sobre privacidad o confidencialidad, propiedad intelectual, flujo de datos externos y criptografía aplicables a las prácticas de tecnología de información de la organización.

e) Comercio electrónico

La gerencia deberá asegurar que se establezcan contratos formales, para determinar acuerdos entre socios comerciales sobre procesos de comunicación, así como sobre estándares de mensajes de transacción, seguridad y almacenamiento de datos. Cuando se realicen operaciones de intercambio en Internet, la gerencia deberá imponer adecuados controles para asegurar el cumplimiento de leyes locales y costumbres en un ámbito mundial.

f) Cumplimiento con los contratos de seguros

La gerencia deberá asegurar la identificación y el continuo cumplimiento de los requerimientos de los contratos de seguros.

3.2.1.9 Evaluación de riesgos

El objetivo principal de la estructura que satisface los requerimientos de negocio de asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, se hace posible a través de la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos, y toma en consideración:

- Los diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.)
- El alcance: global o de sistemas específicos
- La actualización de evaluación de riegos
- La metodología de evaluación de riesgos
- La medición de riesgos cualitativos y/o cuantitativos
- El plan de acción de riesgos

Tabla XI. **Criterios y recursos en la evaluación de riesgos**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	Integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
S	S	P	P	P	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Evaluación de riesgos del negocio

La gerencia deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes, para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos, tanto a un nivel global, como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos, utilizando los resultados de auditorías, inspecciones e incidentes identificados.

b) Enfoque de evaluación de riesgos

La gerencia deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología que va a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

c) Identificación de riesgos

La evaluación de riesgos deberá orientarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.

d) Medición de riesgos

El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo, al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

e) Plan de acción contra riesgos

El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos, para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

f) Aceptación de riesgos

El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, que depende de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de cuán económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

3.2.1.10 Administración de proyectos

El objetivo que satisface los requerimientos de negocio de establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión, se hace posible a través de la identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido, y toma en consideración:

- La propiedad de los proyectos
- El involucramiento de los usuarios
- La estructuración jerárquica de tareas y los puntos de revisión
- La asignación de responsabilidades
- La aprobación de fases y proyecto
- Los presupuestos de costos y horas hombre
- Los planes y metodología de aseguramiento de calidad

Tabla XII. **Criterios y recursos para la administración**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	Cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P							¤	¤	¤	¤	

Objetivos de control detallados

a) Marco de referencia para la administración de proyectos

La gerencia deberá establecer un marco de referencia general para la administración de proyectos, que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos que va a ser adoptada y aplicada para cada proyecto emprendido.

La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

b) Participación del departamento usuario en la iniciación de proyectos

El marco de referencia de la administración de proyectos de la organización deberá fomentar la participación del departamento usuario afectado en la definición y autorización de cualquier proyecto de desarrollo, implementación o modificación.

c) Miembros y responsabilidades del equipo del proyecto

El marco de referencia de administración de proyectos de la organización deberá especificar las bases para asignar a los miembros del personal al proyecto, y definir las responsabilidades y autoridades de los miembros del equipo del proyecto.

d) Definición del proyecto

El marco de referencia de administración de proyectos de la organización deberá generar la creación de un estatuto claro por escrito, que defina la naturaleza y el alcance de cada proyecto de implementación antes de que los trabajos del mismo sean iniciados.

e) Aprobación del proyecto

El marco de referencia de administración de proyectos de la organización deberá asegurar que, para cada proyecto propuesto, la alta gerencia de la organización revise los reportes de los estudios de factibilidad relevantes, como una base para fundamentar la decisión de proceder con el proyecto.

f) Aprobación de las fases del proyecto

El marco de referencia de administración de proyectos de la organización deberá disponer que los gerentes designados para las funciones del usuario y de los servicios de información aprueben el trabajo realizado en cada fase del ciclo antes de iniciar los trabajos de la siguiente fase.

g) Plan maestro del proyecto

La gerencia deberá asegurar que, para cada proyecto aprobado, se cree un plan maestro adecuado que mantenga el control del proyecto a través de todo su desarrollo e incluya un método de monitoreo del tiempo y los costos incurridos durante su vida.

h) Plan de aseguramiento de la calidad de sistemas

La gerencia deberá asegurar que la implementación de un sistema nuevo o modificado incluya la preparación de un plan de calidad que sea integrado posteriormente al plan maestro del proyecto y que sea formalmente revisado y acordado por todas las partes interesadas.

i) Planeación de métodos de aseguramiento

Las tareas de aseguramiento deberán ser definidas durante la fase de planeación del marco de referencia de administración de proyectos. Las tareas de aseguramiento deberán apoyar la acreditación de sistemas nuevos o modificados y garantizar que los controles internos y los dispositivos de seguridad cumplan con los requerimientos necesarios.

j) Administración formal de riesgos de proyectos

La gerencia deberá implementar un programa de administración formal de riesgos de proyectos, para eliminar o minimizar los riesgos asociados con proyectos individuales (por ejemplo, identificación y control de áreas o eventos que tengan el potencial de causar cambios no deseados).

k) Plan de prueba

El marco de referencia de administración de proyectos de la organización deberá requerir la creación de un plan de pruebas para cada proyecto de desarrollo, implementación y modificación.

l) Plan de entrenamiento

El marco de referencia de administración de proyectos de la organización deberá requerir la creación de un plan de entrenamiento para cada proyecto de desarrollo, implementación y modificación.

m) Plan de revisión post – implementación

El marco de referencia de administración de proyectos de la organización deberá disponer que, como parte integral de las actividades del equipo del proyecto, se desarrolle un plan de revisión post - implementación para cada sistema de información nuevo o modificado, con la finalidad de determinar si el proyecto ha generado los beneficios planeados.

3.2.1.11 Administración de calidad

El objetivo que satisface los requerimientos de negocio de satisfacer los requerimientos del cliente, se hace posible a través de la planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización , y toma en consideración:

- La estructura del plan de calidad
- La responsabilidades de aseguramiento de la calidad
- La metodología del ciclo de vida de desarrollo de sistemas
- Las pruebas y documentación de sistemas y programas
- Las revisiones y reporte de aseguramiento de calidad

Tabla XIII. **Criterios y recursos para la administración de calidad**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P		P			S		¤	¤			

Objetivos de control detallado

a) Plan general de calidad

La alta gerencia deberá desarrollar y mantener regularmente un plan general de calidad basado en los planes organizacionales y de tecnología de información a largo plazo. El plan deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

b) Enfoque de aseguramiento de calidad

La gerencia deberá establecer un enfoque estándar respecto al aseguramiento de calidad, que cubra tanto las actividades de aseguramiento de calidad generales como las específicas de un proyecto. El enfoque deberá determinar el (los) tipo(s) de actividades de aseguramiento de calidad (tales como revisiones, auditorías, inspecciones, etc.) que deben realizarse para

alcanzar los objetivos del plan general de calidad. Asimismo deberá requerir una revisión específica de aseguramiento de calidad.

c) Planeación del aseguramiento de calidad

La gerencia deberá implementar un proceso de planeación de aseguramiento de calidad, para determinar el alcance y la duración de las actividades de aseguramiento de calidad.

d) Revisión del aseguramiento de la calidad sobre el cumplimiento de estándares y procedimientos de la función de servicios de información

La gerencia deberá asegurar que las responsabilidades asignadas al personal de aseguramiento de calidad incluyan una revisión del cumplimiento general de los estándares y procedimientos de la función de servicios de información.

e) Metodología del ciclo de vida de desarrollo de sistemas

La alta gerencia de la organización deberá definir e implementar estándares de sistemas de información y adoptar una metodología del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información computarizados y tecnología afín.

La metodología del ciclo de vida de desarrollo de sistemas elegida deberá ser la apropiada para los sistemas que van a ser desarrollados, adquiridos, implementados y mantenidos.

f) Metodología del ciclo de vida de desarrollo de sistemas para cambios mayores a la tecnología actual

En el caso de requerirse cambios mayores a la tecnología actual, la gerencia deberá asegurar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas, como en el caso de adquisición de nueva tecnología.

g) Actualización de la metodología del ciclo de vida de desarrollo de sistemas

La alta gerencia deberá implementar una revisión periódica de su metodología del ciclo de vida de desarrollo de sistemas, para asegurar que incluya técnicas y procedimientos actuales generalmente aceptados.

h) Coordinación y comunicación

La gerencia deberá establecer un proceso para asegurar la coordinación y comunicación estrecha entre los clientes de la función de servicios de información y los implementadores de sistemas. Este proceso deberá lograr o hacer que los métodos estructurados que utilicen la metodología del ciclo de vida de desarrollo de sistemas aseguren la provisión de soluciones de tecnología de información de calidad, que satisfagan las demandas de negocio.

La gerencia deberá promover una organización que se caracterice por la estrecha cooperación y comunicación a lo largo del ciclo de vida de desarrollo de sistemas.

i) Marco de referencia de adquisición y mantenimiento para la infraestructura de tecnología

Deberá establecerse un marco de referencia general referente a la adquisición y mantenimiento de la infraestructura de tecnología. Los diferentes pasos que deben ser seguidos respecto a la infraestructura de tecnología (tales como adquisición; programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y aplicación de correcciones), deberán estar regidos por y mantenerse en línea con el marco de referencia para la adquisición y mantenimiento de la infraestructura de tecnología.

j) Relaciones con terceras partes como implementadores

La Gerencia deberá implementar un proceso para asegurar las buenas relaciones de trabajo con terceras partes como implementadores externos.

Dicho proceso deberá disponer que el usuario y el implementador estén de acuerdo sobre los criterios de aceptación, el manejo de cambios, los problemas durante el desarrollo, las funciones de los usuarios, las instalaciones, las herramientas, el software, los estándares y los procedimientos.

k) Estándares para la documentación de programas

La metodología del ciclo de vida de desarrollo de sistemas deberá incorporar estándares para la documentación de programas que hayan sido impuestos y comunicados al personal interesado.

La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema de información o de los proyectos de modificación coincida con estos estándares.

l) Estándares para pruebas de programas

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar las unidades de software y los programas agregados, creados como parte de cada proyecto de desarrollo o modificación de sistemas de información.

m) Estándares para pruebas de sistemas

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requerimientos de pruebas, verificación, documentación y retención para probar el sistema total, como parte de cada proyecto de desarrollo o modificación de sistemas de información.

n) Pruebas piloto / en paralelo

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe definir las condiciones bajo las cuales deberán conducirse las pruebas piloto o en paralelo de sistemas nuevos y/o actuales.

o) Documentación de las pruebas del sistema

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe disponer, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información, que se conserve la documentación de los resultados de las pruebas del sistema.

p) Evaluación del aseguramiento de la calidad sobre el cumplimiento de estándares de desarrollo

El enfoque de aseguramiento de calidad de la organización deberá requerir que una revisión post - implementación de un sistema de información operacional evalúe si el equipo encargado del proyecto cumplió con las estipulaciones de la metodología del ciclo de vida de desarrollo de sistemas.

q) Revisión del aseguramiento de calidad sobre el logro de los objetivos de la función de servicios de información

El enfoque de aseguramiento de calidad deberá incluir una revisión de hasta qué punto los sistemas particulares y las actividades de desarrollo de aplicaciones han alcanzado los objetivos de la función de servicios de información.

r) Métricas de calidad

La gerencia deberá definir y utilizar métricas para medir los resultados de actividades, evaluando si las metas de calidad han sido alcanzadas.

s) Reportes de revisiones de aseguramiento de calidad

Los reportes de revisiones de aseguramiento de calidad deberán ser preparados y enviados a la Gerencia de los departamentos usuarios y de la función de servicios de información.

3.2.2 Objetivos de adquisición e implementación

3.2.2.1 Identificación de soluciones

Satisface los requerimientos de negocio de asegurar el mejor enfoque para cumplir con los requerimientos del usuario, se hace posible a través de un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios, y toma en consideración:

- La definición de requerimientos de información
- Los estudios de factibilidad (de costo-beneficio, alternativas, etc.)
- La arquitectura de información
- La seguridad con relación de costo-beneficio favorable
- Las pistas de auditoría
- La contratación de terceros
- La aceptación de instalaciones y tecnología

Tabla XIV. **Criterios y recursos para identificar soluciones**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	S								¤	¤	¤	

Objetivos de control detallados

a) Definición de requerimientos de información

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los requerimientos del negocio ya satisfechos por el sistema actual y que van a ser satisfechos por el sistema nuevo propuesto o modificado (*software*, datos e infraestructura), estén claramente definidos antes de aprobar cualquier proyecto de desarrollo, implementación o modificación.

La metodología del ciclo de vida de desarrollo de sistemas deberá exigir que los requerimientos de las soluciones funcionales y operacionales sean especificados, incluyendo desempeño, protección, confiabilidad, compatibilidad, seguridad y legislación.

b) Formulación de acciones alternativas

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proveer el análisis de las acciones alternativas, que deberán satisfacer los requerimientos del negocio, establecidos para un sistema nuevo o modificado.

c) Formulación de estrategias de adquisición

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un plan de estrategia de adquisición, que define si el software será "adquirido del mostrador", desarrollados internamente, a través de contratación o mediante una combinación de éstos.

d) Requerimientos de servicios de terceros

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular la evaluación de requerimientos y las especificaciones para una solicitud de propuesta, cuando se negocie con un proveedor de servicios externo.

e) Estudio de factibilidad tecnológica

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un examen de factibilidad tecnológica de cada alternativa, con la finalidad de satisfacer los requerimientos de negocio establecidos para el desarrollo de un proyecto propuesto de cualquier sistema nuevo o modificado.

f) Estudio de factibilidad económica

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe generar, en cada proyecto de desarrollo, la implementación y modificación de sistemas de información propuesto, el análisis de los costos y los beneficios asociados con cada alternativa considerada, para satisfacer los requerimientos del negocio establecidos.

g) Arquitectura de información

La gerencia deberá asegurar que se tome en consideración el modelo de datos de la empresa al definir las soluciones y analizar la factibilidad de las mismas.

h) Reporte de análisis de riesgos

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, en cada proyecto de desarrollo, la implementación y modificación de sistemas de información propuesto, el análisis y la documentación de las amenazas a la seguridad, puntos de impacto y debilidad, así como protecciones factibles de seguridad y control interno, con la finalidad de reducir o eliminar el riesgo identificado.

Esto deberá llevarse a cabo en línea con el marco de referencia general de evaluación de riesgos.

i) Controles de seguridad económicos

La gerencia deberá asegurar que los costos y beneficios de seguridad sean examinados cuidadosamente en términos monetarios y no monetarios, para garantizar que los costos de los controles no excedan a los beneficios. La decisión requerirá la firma de aprobación formal de la gerencia.

j) Diseño de pistas de auditoría

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que existan mecanismos adecuados para pistas de auditoría, o que dichos mecanismos puedan ser desarrollados para la solución identificada y seleccionada. Los mecanismos deberán proporcionar la capacidad de proteger datos sensitivos (Ej. identificación de usuarios contra divulgación o mal uso).

k) Ergonomía

La gerencia deberá asegurar que los proyectos de desarrollo, implementación y cambios emprendidos por la función de servicios de información, tomen en consideración los aspectos ergonómicos asociados con la introducción de soluciones automatizadas.

l) Selección del *software* del sistema

La gerencia deberá asegurar que la función de servicios de información cumpla con un procedimiento estándar para identificar todos los programas de *software* potenciales, que deberán satisfacer sus requerimientos operacionales.

m) Control de abastecimiento

La gerencia deberá desarrollar e implementar un enfoque central de abastecimientos que describa un conjunto común de procedimientos y estándares que van a ser seguidos en la adquisición de *hardware, software* y servicios relacionados con la tecnología de información. Los productos deberán ser revisados y probados antes de su utilización y pago.

n) Adquisición de productos de *software*

La adquisición de productos de *software* deberá seguir las políticas de adquisición de la organización.

o) Mantenimiento de *software* de terceras partes

La gerencia deberá asegurar que, para el *software* con licencia adquirido a terceras partes, los proveedores cuenten con los procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de *software*. Deberá tomarse en consideración el soporte del producto en cualquier acuerdo de mantenimiento relacionado con el producto entregado.

p) Contratos de programación de aplicaciones

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los servicios de programación contratados estén justificados con una solicitud de servicios por escrito por parte de un miembro designado de la función de servicios de información. El contrato deberá estipular que el *software*, la documentación y otros elementos

entregables estén sujetos a pruebas y revisiones antes de ser aceptados. Además, deberá asegurar que los productos finales terminados por los servicios de programación contratados sean revisados y probados de acuerdo con los estándares definidos por el grupo de aseguramiento de calidad de la función de servicios de información y otras partes interesadas (como usuarios, administradores de proyecto, etc.), antes de pagar por el trabajo y aprobar el producto final.

Las pruebas, que deberán ser incluidas en las especificaciones del contrato, deberán consistir en pruebas del sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de afinación y desempeño, pruebas de regresión, pruebas de aceptación del usuario y, finalmente, pruebas piloto del sistema total, con la finalidad de evitar fallas no esperadas del mismo.

q) Aceptación de instalaciones

La gerencia deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para las instalaciones que van a ser proporcionadas, el cual defina los procedimientos y criterios de aceptación. Además, deberán llevarse a cabo pruebas de aceptación, para garantizar que el acomodo y el medio cumplan con los requerimientos especificados en el contrato.

r) Aceptación de tecnología

La gerencia deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para la tecnología específica a ser proporcionada, el cual defina los procedimientos y criterios de aceptación.

Además, las pruebas de aceptación establecidas en el plan, deberán incluir inspección, pruebas de funcionalidad y seguimiento de cargas de trabajo.

3.2.2.2 Adquisición y mantenimiento de software

El objetivo que satisface los requerimientos de negocio de proporcionar funciones automatizadas que soporten efectivamente al negocio, se hace posible a través de la definición de declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros, y toma en consideración:

- Los requerimientos de usuarios
- Los requerimientos de archivo, entrada, proceso y salida
- El interfase usuario – máquina
- La personalización de paquetes
- Las pruebas funcionales
- Los controles de aplicación y requerimientos funcionales
- La documentación

Tabla XV. **Criterios y recursos para adquisición y mantenimiento de software**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P		S		S	S			¤			

Objetivos de control detallados

a) Métodos de diseño

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que sean aplicados a técnicas y procedimientos apropiados, incluyendo una estrecha relación con los usuarios del sistema, en la creación de las especificaciones de diseño para cada nuevo proyecto de desarrollo de sistemas de información, y verificar las especificaciones del diseño contra los requerimientos del usuario.

b) Cambios significativos a sistemas actuales

La gerencia deberá asegurar que, en caso de presentarse la necesidad de realizar modificaciones significativas a los sistemas actuales, se siga un proceso de desarrollo similar al utilizado en el desarrollo de sistemas nuevos.

c) Aprobación del diseño

La metodología del ciclo de vida de desarrollo de sistemas de la organización requerirá que las especificaciones de diseño para todos los proyectos de desarrollo y modificación de sistemas de información, sean revisados y aprobados por la Gerencia, por los departamentos usuarios afectados y por la alta gerencia de la organización, cuando esto sea pertinente.

d) Definición y documentación de requerimientos de archivos

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la aplicación de un procedimiento apropiado para la definición y documentación del formato de los archivos para cada proyecto de desarrollo y la modificación de sistemas de información. Este procedimiento deberá garantizar el respeto a las reglas de diccionario de datos.

e) Especificaciones de programas

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la preparación de especificaciones detalladas por escrito, de los programas para cada proyecto de desarrollo o modificación de sistemas de información. Además, la metodología deberá garantizar que las especificaciones de los programas correspondan a las especificaciones del diseño del sistema.

f) Diseño para la recopilación de datos fuente

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la especificación de mecanismos adecuados, para la recopilación y entrada de datos para cada proyecto de desarrollo y modificación de sistemas de información.

g) Definición y documentación de requerimientos de entrada de datos

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados, para definir y documentar los requerimientos de entrada de datos para cada proyecto de desarrollo o modificación de sistemas de información.

h) Definición de interfases

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que se especifiquen, diseñen y documenten apropiadamente todas las interfases internas y externas.

i) Interfase usuario-máquina

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar el desarrollo de una interfase entre el usuario y la máquina fácil de utilizar, y que sea capaz de auto documentarse (por medio de funciones de ayuda en línea).

j) Definición y documentación de requerimientos de procesamiento

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de procesamiento, para cada proyecto de desarrollo o modificación de sistemas de información.

k) Definición y documentación de requerimientos de salida de datos

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requerimientos de salida de datos para cada proyecto de desarrollo, o la modificación de sistemas de información

l) Controlabilidad

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se especifiquen los mecanismos adecuados, para garantizar que se identifiquen los requerimientos de seguridad y control internos para cada proyecto de desarrollo o modificación de sistemas de información. La metodología deberá asegurar, además, que los sistemas de información estén diseñados para incluir controles de aplicación que garanticen que los datos de entrada y salida estén completos, así como su precisión, oportunidad y autorización. Deberá llevarse a cabo una evaluación de sensibilidad durante el inicio del desarrollo o modificación del sistema.

Los aspectos básicos de seguridad y control interno de un sistema que va a ser desarrollado o modificado deberán ser evaluados junto con el diseño conceptual del mismo, con el fin de integrar los conceptos de seguridad en el diseño, tan pronto como sea posible.

m) Disponibilidad como factor clave de diseño

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que la disponibilidad sea considerada en el proceso de diseño de nuevos o modificados sistemas de información en la fase más temprana posible.

La disponibilidad debe ser analizada y, en caso necesario, incrementada a través de mejoras de mantenimiento y confiabilidad.

n) Consideraciones de integridad de tecnología para *software* de programas de aplicación

La organización deberá establecer procedimientos para asegurar, cuando esto aplique, que los programas de aplicación contengan estipulaciones que verifiquen rutinariamente las tareas realizadas por el *software*, para apoyar el aseguramiento de la integridad de los datos, y el cual haga posible la restauración de la integridad a través de procedimientos de recuperación en reversa u otros medios.

o) Pruebas de *software* de aplicación

Deberán aplicarse pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga y estrés, de acuerdo con el plan de prueba del proyecto y con los estándares de pruebas establecidos, antes de ser aprobado por el usuario. Se deberán aplicar adecuadas medidas de seguridad para prevenir divulgación de información sensitiva durante las pruebas.

p) Materiales de consulta y soporte para usuarios

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen manuales de referencia y soporte para usuarios adecuados (preferiblemente en formato electrónico), como parte de cada proyecto de desarrollo o modificación de sistemas de información

q) Reevaluación del diseño del sistema

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que el diseño del sistema sea reevaluado siempre que ocurran discrepancias técnicas y/o lógicas durante el desarrollo o mantenimiento del sistema.

3.2.2.3 Adquisición y mantenimiento de arquitectura de tecnología

Satisface los requerimientos de negocio de proporcionar las plataformas apropiadas para soportar aplicaciones de negocios, se hace posible a través de la evaluación del desempeño de *hardware y software*, la provisión de mantenimiento preventivo de *hardware* y la instalación, seguridad y control del *software* del sistema.

Y toma en consideración:

- La evaluación de tecnología
- El mantenimiento preventivo de *hardware*
- La seguridad del *software* de sistema, instalación, mantenimiento y control sobre cambios

Tabla XVI. **Criterios y recursos para la adquisición de tecnología**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	Confiabilidad		Recursos	aplicación	tecnología	instalaciones	datos
P	P		S							¤		

Objetivos de control detallados

a) Valuación de nuevo *hardware y software*

Deberán establecerse procedimientos para evaluar el impacto de nuevo *hardware y software* sobre el rendimiento del sistema en general.

b) Mantenimiento preventivo para *hardware*

La gerencia de la función de servicios de información deberá calendarizar el mantenimiento rutinario y periódico del *hardware*, con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

c) Seguridad del *software* del sistema

La gerencia de la función de servicios de información deberá asegurar que la instalación del *software* del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

d) Instalación del *software* del sistema

Deberán implementarse procedimientos para asegurar que el *software* del sistema sea instalado, de acuerdo con el marco de referencia de adquisición y mantenimiento de infraestructura de tecnología. Las pruebas deberán ser llevadas a cabo antes de autorizarse su utilización en el ambiente de producción.

e) Mantenimiento del *software* del sistema

Deberán implementarse procedimientos para asegurar que el *software* del sistema sea mantenido de acuerdo con el marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

f) Controles para cambios del *software* del sistema

Deberán implementarse procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la organización.

3.2.2.4 Desarrollo y mantenimiento

Satisface los requerimientos de negocio de asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas, se hace posible a través de un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento, y toma en consideración:

- Los procedimientos y controles de usuarios
- Los procedimientos y controles operacionales
- Los materiales de entrenamiento

Tabla XVII. **Criterios y recursos en el desarrollo y mantenimiento**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P		S		S	S		¤	¤	¤	¤	

Objetivos de control detallados

a) Requerimientos operacionales y niveles de servicios futuros

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la definición oportuna de requerimientos operacionales y niveles de servicios futuros.

b) Manual de procedimientos para usuario

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen y actualicen manuales adecuados de procedimientos para los usuarios, como parte de cada proyecto de desarrollo o modificación de sistemas de información.

c) Manual de operaciones

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se prepare y se mantenga actualizado un manual de operaciones adecuado, como parte de cada proyecto de desarrollo o modificación de sistemas de información.

d) Material de entrenamiento

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se desarrollen materiales de entrenamiento adecuados, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información.

Estos materiales deberán enfocarse al uso del sistema en la práctica diaria.

3.2.2.5 Instalación y acreditación de sistemas

Satisface los requerimientos de negocio de verificar y confirmar que la solución sea adecuada para el propósito deseado, se hace posible a través de la realización de una migración de instalación, conversión y plan de aceptación, adecuadamente formalizados, y toma en consideración:

- La capacitación
- La conversión / carga de datos
- Las pruebas específicas
- La acreditación
- Las revisiones post implementación

Tabla XVIII. **Criterios y recursos para la instalación y acreditación de sistemas**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	Cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P			S	S				¤	¤	¤	¤	¤

Objetivos de control detallados

a) Entrenamiento

El personal de los departamentos usuarios afectados y el grupo de operaciones de la función de servicios de información deberán estar entrenados de acuerdo con el plan de entrenamiento definido y los materiales relacionados, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información.

b) Adecuación del desempeño del *software* de aplicación

La medición (optimización) del desempeño del *software* de aplicación deberá establecerse como una parte integral de la metodología del ciclo de vida de desarrollo de sistemas de la organización, para predecir los recursos requeridos para operar *software* nuevo o significativamente modificado.

c) Conversión

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, como parte de cada proyecto de desarrollo, la implementación o modificación de sistemas de información, que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo de acuerdo con el plan preestablecido.

d) Pruebas de cambios

La gerencia deberá asegurar que los cambios sean probados por un grupo de prueba independiente (distinto al de los desarrolladores), de acuerdo con la evaluación de impacto y recursos en un ambiente de prueba separado, antes de comenzar su uso en el ambiente de operación regular.

También deberán desarrollarse planes de respaldo. Las pruebas de aceptación deberán llevarse a cabo en un ambiente representativo del ambiente operacional futuro (por ejemplo, condiciones similares de seguridad, controles internos, cargas de trabajo, etc.)

e) Criterios y desempeño de pruebas en paralelo piloto

Deben establecerse procedimientos para asegurar que las pruebas piloto o en paralelo sean llevadas a cabo, de acuerdo con un plan preestablecido y que los criterios para la terminación del proceso de pruebas sean especificados con anterioridad.

f) Prueba de aceptación final

Los procedimientos deberán asegurar, como parte de las pruebas de aceptación final o de aseguramiento de calidad de sistemas de información nuevos o modificados, una evaluación y aprobación formal de los resultados de las pruebas por parte de la gerencia de los departamentos usuarios afectados y de la función de servicios de información.

Las pruebas deben cubrir todos los componentes del sistema de información (*software* de aplicación, instalaciones, tecnología, procedimientos de usuarios).

g) Pruebas y acreditación de seguridad

La gerencia deberá definir e implementar procedimientos para asegurar que la gerencia de operaciones y la gerencia usuaria aceptan formalmente los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

h) Prueba operacional

La gerencia deberá asegurar que, antes de poner el sistema en operación, el usuario o custodio designado (la parte designada para correr el sistema en nombre del usuario), valide su operación como un producto completo, bajo condiciones similares a las del ambiente de aplicación, y en la manera en la que el sistema será operado en un ambiente de producción.

i) Paso a producción

La gerencia deberá definir e implementar procedimientos formales para controlar la entrega del sistema de desarrollo a pruebas y a operación. Los ambientes respectivos deberán separarse y protegerse apropiadamente.

j) Evaluación de la satisfacción de los requerimientos del usuario

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se realice una revisión post - implementación de los requerimientos operacionales del sistema de información (por ejemplo, capacidad, desempeño de procesamiento a través del sistema etc.), con el fin de evaluar si las necesidades del usuario están siendo satisfechas por el mismo.

k) Revisión gerencial post – implementación

La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que una revisión post - implementación del sistema de información operacional evalúe, y reporte si el sistema proporcionó los beneficios esperados de la manera más económica.

3.2.2.6 Administración de cambios

Satisface los requerimientos de negocio de minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores, se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual, y toma en consideración:

- La identificación de cambios
- Los procedimientos de categorización, priorización y emergencia
- La evaluación del impacto
- La autorización de cambios
- El manejo de liberación
- La distribución de software

Tabla XIX. **Criterios y recursos para la administración de cambios**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		Recursos	aplicación	tecnología	instalaciones	Datos
P	P		P	P		S		¤	¤	¤	¤	¤

Objetivos de control detallado

a) Inicio y control de requisiciones de cambio

La gerencia deberá asegurar que todas las requisiciones de cambios, tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios.

Las solicitudes deberán categorizarse, priorizarse y establecerse los procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estatus de su solicitud.

b) Evaluación del impacto

Deberá establecerse un procedimiento para asegurar que todas las requisiciones de cambio sean evaluadas en una forma estructurada, en cuanto a todos los posibles impactos sobre el sistema operacional y su funcionalidad.

c) Control de cambios

La gerencia deberá asegurar que la administración de cambios, así como el control y la distribución de *software* sean integrados apropiadamente en un sistema completo de administración de configuración.

d) Documentación y procedimientos

El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

e) Mantenimiento autorizado

La gerencia deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados, para evitar riesgos de accesos no autorizados a los sistemas automatizados.

f) Política de liberación de *software*

La gerencia deberá garantizar que la liberación de *software* esté regida por procedimientos formales, que aseguren la aprobación, el empaque, las pruebas de regresión, entrega, etc.

g) Distribución de *software*

Deberán establecerse medidas de control específicas para asegurar la distribución del elemento de software correcto al lugar correcto, con integridad y de manera oportuna con pistas de auditoría adecuadas.

3.2.3 Entrega de servicios y soporte

3.2.3.1 Niveles de servicio

Satisface los requerimientos de negocio de establecer una comprensión común del nivel de servicio requerido, se hace posible a través de el establecimiento de convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio.

Y toma en consideración:

- Los convenios formales
- La definición de responsabilidades
- Los tiempos y volúmenes de respuesta
- Las dependencias
- Los cargos
- Las garantías de integridad
- Los convenios de confidencialidad

Tabla XX. **Criterios y recursos para la entrega de servicios**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P	S	S	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Marco de referencia para el convenio de nivel de servicio

La alta gerencia deberá establecer un marco de referencia en donde presente la definición de los convenios sobre niveles formales de servicio, y determine el contenido mínimo: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia, recuperación, nivel mínimo aceptable de funcionalidad del sistema, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos.

El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y la cantidad de servicios ofrecida y los usuarios deberán ajustar los servicios solicitados a los límites acordados.

b) Aspectos sobre los convenios de nivel de servicio

Deberá lograrse un acuerdo explícito sobre los aspectos que el convenio de nivel de servicios deberá tener. El convenio de nivel de servicio deberá cubrir, por lo menos, los siguientes aspectos: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados a los usuarios, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambios.

c) Procedimientos de desempeño

Deberán definirse procedimientos que aseguren que la manera y responsabilidades sobre las relaciones que rigen el desempeño, por ejemplo, convenios de confidencialidad, entre todas las partes involucradas, sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

d) Monitoreo y reporte

La gerencia de la función de servicios de información deberá designar a un gerente de nivel de servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

e) Revisión de convenios y contratos de nivel de servicio

La gerencia deberá implementar un proceso de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de servicios como terceras partes.

f) Elementos sujetos a cargo

Deberán incluirse provisiones para elementos sujetos a cargo en los acuerdos de niveles de servicio, para hacer posible comparaciones y decisiones de niveles de servicio contra su costo.

g) Programa de mejoramiento del servicio

La gerencia deberá implementar un proceso para asegurar que los usuarios y los gerentes de nivel de servicio concuerden regularmente en un programa de mejoramiento del servicio, con el fin de dar seguimiento a mejoras al nivel de servicio, cuyo costo esté justificado.

3.2.3.2 Servicios prestados por terceros

El objetivo que satisface los requerimientos de negocio de asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos, se hace posible a través de medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización.

Y toma en consideración:

- Los acuerdos de servicio con terceras partes
- Los acuerdos de confidencialidad
- Los requerimientos legales regulatorios
- El monitoreo de la entrega de servicio

Tabla XXI. **Criterios y recursos en los servicios prestados por terceros**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	Cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P	S	S	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Interfases con proveedores

La Gerencia deberá asegurar que todos los servicios prestados por terceros sean propiamente identificados y que las interfases técnicas y organizacionales con los proveedores sean documentadas.

b) Relaciones de dueños

La gerencia de la organización del cliente deberá designar un dueño que sea responsable de asegurar la calidad de las relaciones con terceros.

c) Contratos con terceros

La gerencia debe definir procedimientos específicos, para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con un proveedor.

d) Calificación de terceros

La gerencia debe asegurar, en forma previa a su selección, que los terceros potenciales cuentan con las calificaciones adecuadas a través de una evaluación de su capacidad para proporcionar los servicios requeridos.

e) Contratos con fuentes externas

Deberán definirse procedimientos organizacionales específicos, para asegurar que el contrato entre la organización y el proveedor de la administración de instalaciones esté basado en niveles de procesamiento

requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones, según sea apropiado.

f) Continuidad de servicios

Respecto al aseguramiento de la continuidad de los servicios, la gerencia deberá considerar el riesgo de negocios relacionado con la participación de terceros en términos de incertidumbre legal, y con el concepto de interés sobre la continuidad y negociar contratos en depósito.

g) Relaciones de seguridad

En cuanto a las relaciones con los proveedores de servicios como terceras partes, la gerencia deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de no - revelación) sean identificados, declarados explícitamente y acordados; que éstos concuerden con los estándares de negocios universales y estén en línea con los requerimientos legales y regulatorios, incluyendo obligaciones.

h) Monitoreo

La gerencia deberá establecer un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

3.2.3.3 Administración de desempeño y capacidad

Satisface los requerimientos de negocio de asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado, se hace posible a través de controles de manejo de capacidad y desempeño que

recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos, y toma en consideración:

- Los requerimientos de disponibilidad y desempeño
- El monitoreo y reporte
- Las herramientas de modelado
- La administración de capacidad
- La disponibilidad de recursos

Tabla XXII. **Criterios y recursos para la administración del desempeño**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P			S					¤	¤	¤	

Objetivos de control detallados

a) Requerimientos de disponibilidad y desempeño

El proceso de administración deberá asegurar que las necesidades de negocio respecto a disponibilidad y desempeño de los servicios de información sean identificadas y convertidas en requerimientos y términos de disponibilidad.

b) Plan de disponibilidad

La gerencia deberá asegurar el establecimiento de un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.

c) Monitoreo y reporte

La gerencia deberá implementar un proceso que asegure que el desempeño de los recursos de tecnología de información sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

d) Herramientas de modelado

La gerencia deberá asegurar que se utilicen las herramientas de modelado apropiadas para producir un modelo del sistema actual, calibrado y ajustado según la carga de trabajo real y que sea preciso dentro de los niveles de carga recomendados. Las herramientas de modelado deberán utilizarse para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad. Deberán llevarse a cabo investigaciones técnicas profundas sobre el *hardware* de los sistemas, y deberán incluirse pronósticos acerca de futuras tecnologías.

e) Manejo proactivo del desempeño

El proceso de administración del desempeño deberá incluir la capacidad de pronóstico, para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado del impacto y magnitud del daño.

f) Pronóstico de carga de trabajo

Deberán establecerse controles para asegurar que se preparen pronósticos de carga de trabajo, con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad.

g) Administración de capacidad de recursos

La gerencia de la función de servicios de información deberá establecer un proceso de planeación para la revisión del desempeño y capacidad del *hardware*, con el fin de asegurar que siempre exista una capacidad justificable económicamente, para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas, prescritas en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

h) Disponibilidad de recursos

La gerencia deberá prevenir que se pierda la disponibilidad de los recursos, mediante la implementación de mecanismos de tolerancia de fallas, mecanismos de asignación equitativa de recursos y la definición de prioridades de tareas.

i) Calendarización de recursos

La gerencia deberá asegurar la adquisición oportuna de la capacidad requerida, tomando en cuenta aspectos como resistencia, contingencia, cargas de trabajo y planes de almacenamiento.

3.2.3.4 Asegurar continuidad de servicio

El objetivo que satisface los requerimientos de negocio de mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, se hace posible a través de tener un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio, y toma en consideración:

- La clasificación de severidad
- El plan documentado
- Los procedimientos alternativos
- El respaldo y recuperación
- Las pruebas y entrenamiento sistemáticos y regulares

Tabla XXIII. **Criterios y recursos para asegurar la continuidad de servicio**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	S			P				¤	¤	¤	¤	¤

Objetivos de control detallados

a) Marco de referencia de continuidad de tecnología de información

La gerencia de la función de servicios de información deberá crear un marco de referencia de continuidad que defina los roles, responsabilidades, el enfoque basado en riesgo, la metodología que va a seguir y las reglas y la estructura para documentar el plan, así como los procedimientos de aprobación.

b) Estrategia y filosofía de continuidad de tecnología de Información

La gerencia deberá garantizar que el Plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa, para asegurar consistencia.

Aun más, el plan de continuidad de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.

c) Contenido del plan de continuidad de tecnología de Información

La gerencia de la función de servicios de información deberá asegurar que se desarrolle un plan escrito que contenga lo siguiente:

- Guías sobre la utilización del plan de continuidad.
- Procedimientos de emergencia para asegurar la integridad de todo el personal afectado.

- Procedimientos de respuesta definidos, para regresar al negocio al estado en que se encontraba antes del incidente o desastre.
- Procedimientos para salvaguardar y reconstruir las instalaciones.
- Procedimientos de coordinación con las autoridades públicas.
- Procedimientos de comunicación con los interesados: empleados, clientes clave, proveedores críticos, accionistas y gerencia.
- Información crítica sobre grupos de continuidad, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.

d) Minimización de requerimientos de continuidad de tecnología de información.

La gerencia de servicios de información deberá establecer procedimientos y guías para minimizar los requerimientos de continuidad, respecto al personal, instalaciones, *hardware, software*, equipo, formatos, consumibles y mobiliario.

e) Mantenimiento plan de continuidad de tecnología de información

La gerencia de servicios de información deberá proveer procedimientos de control de cambios, para asegurar que el plan de continuidad se mantenga actualizado y refleje requerimientos de negocio actuales. Esto requiere de procedimientos de mantenimiento del plan de continuidad alineados con el cambio, la administración y los procedimientos de recursos humanos.

f) Pruebas del plan de continuidad de tecnología de información

Para contar con un plan efectivo de continuidad, la gerencia necesita evaluar su adecuación de manera regular; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.

g) Capacitación sobre el plan de continuidad de tecnología de información

La metodología de continuidad para desastres deberá asegurar que todas las partes interesadas reciban sesiones de entrenamiento regulares respecto a los procedimientos que deben ser seguidos en caso de un incidente o un desastre.

h) Distribución del plan de continuidad de tecnología de información

Debido a la naturaleza sensitiva de la información del plan de continuidad, dicha información deberá ser distribuida sólo al personal autorizado y mantenerse bajo adecuadas medidas de seguridad para evitar su divulgación.

Consecuentemente, algunas secciones del plan deberán ser distribuidas sólo a las personas, cuyas actividades necesiten el conocimiento de dicha información.

i) Procedimientos de respaldo de procesamiento para departamentos usuarios

La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.

j) Recursos críticos de tecnología de información

El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos, así como los tiempos necesarios para la recuperación, después de que se presenta un desastre.

k) Centro de cómputo y *hardware* de respaldo

La gerencia deberá asegurar que la metodología de continuidad incorpora la identificación de alternativas relativas al centro de cómputo y al *hardware* de respaldo, así como una selección alternativa final. En caso de aplicar, deberá establecerse un contrato formal para este tipo de servicios.

l) Procedimiento de refinamiento del plan de continuidad

Dada una exitosa reanudación de la función de servicios de información, después de un desastre, la gerencia de servicios de información deberá establecer procedimientos para evaluar lo adecuado del plan, y actualizarlo de acuerdo con los resultados de dicha evaluación.

3.2.3.5 Garantizar seguridad de sistemas

Es el objetivo que satisface los requerimientos de negocio de salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, se hace posible a través de controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados, y toma en consideración:

- La autorización
- La autenticación
- El acceso
- Los perfiles e identificación de usuarios
- La administración de llaves criptográficas
- El manejo, reporte y seguimiento de incidentes
- La Prevención y detección de virus
- Los *Firewalls*

Tabla XXIV. **Criterios y recursos para garantizar la seguridad de los sistemas**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
		P	P	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallado

a) Administrar medidas de seguridad

La seguridad en tecnología de información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye:

- traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología
- implementar el plan de seguridad de tecnología de información
- actualizar el plan de seguridad de tecnología de información, para reflejar cambios en la configuración de tecnología
- evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información;
- monitorear la implementación del plan de seguridad de tecnología de información;

- alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos

b) Identificación, autenticación y acceso

El acceso lógico y el uso de los recursos de TI deberá restringirse, a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema (redes) tengan acceso a los recursos de cómputo; de igual forma deberá minimizar la necesidad de firmas de entrada múltiples que van a ser utilizadas por usuarios autorizados. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).

c) Seguridad de acceso a datos en línea

En un ambiente de tecnología de información en línea, la gerencia de la función de servicios de información deberá implementar procedimientos, que esten de acuerdo con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

d) Administración de cuentas de usuario

La gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal, que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

e) Revisión gerencial de cuentas de usuario

La gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

f) Control de usuarios sobre cuentas de usuario

Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información, para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

g) Vigilancia de seguridad

La administración de seguridad de la función de servicios de información debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

h) Clasificación de datos

La gerencia deberá asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aun los datos que requieran "no protección", deberán contar con una decisión formal que les asigne dicha clasificación.

i) Administración centralizada de identificación y derechos de acceso

Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

j) Reportes de violación y de actividades de seguridad

La administración de la función de servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular, para identificar y resolver incidentes que involucren actividades no autorizadas.

El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

k) Manejo de incidentes

La gerencia deberá implementar la capacidad de manejar incidentes de seguridad computacional, y dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras.

Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes, para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

l) Reacreditación

La gerencia deberá asegurar que se lleve a cabo periódicamente una reacreditación de seguridad por ejemplo, a través de equipos de personal técnico, con el fin de conservar al día el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.

m) Confianza en contrapartes

Las políticas organizacionales deberán asegurar que se instrumenten prácticas de control, para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas. Esto puede lograrse mediante el intercambio confiable de *passwords*, dispositivos de seguridad o llaves criptográficas.

n) Autorización de transacciones

Las políticas organizacionales deberán asegurar que, en donde sea apropiado, sean instrumentados controles para proporcionar autenticidad de transacciones. Esto requiere el empleo de técnicas criptográficas para "firmar" y verificar transacciones.

o) No negación

Las políticas organizacionales deberán asegurar que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes y que se instrumenten controles para proporcionar no negación (*non repudiation*) de origen o destino, prueba de envío (*proof of submission*), y recibo de transacciones. Esto puede ser implementado a través de firmas digitales, registro de tiempos y terceros confiables.

p) Sendero seguro

Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (*trusted paths*). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, *passwords* y llaves criptográficas.

Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

q) Protección de funciones de seguridad

Todo el *hardware y software* relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones, para proteger su integridad y contra divulgación de sus claves secretas.

Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

r) Administración de llaves criptográficas

La gerencia deberá definir e implementar procedimientos y protocolos que van a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas contra modificaciones y divulgación no autorizada. Si una llave se encuentra comprometida (en riesgo), la gerencia deberá asegurarse de que esta información se hace llegar

a todas las partes interesadas, a través de un listado de revocación de certificados o mecanismos similares.

s) Prevención, detección y corrección de *software* "malicioso"

Respecto al *software* malicioso, tal como los virus computacionales o caballos de troya, la gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

t) Arquitectura de *firewalls* y conexión a redes públicas

Si existe conexión con internet u otras redes públicas en la organización, se deberá contar con sistemas *Firewall* adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos.

Deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones, y deberá proteger en contra de negación o ataques de servicio.

u) Protección de valores electrónicos

La gerencia debe proteger consistentemente la integridad de todas las tarjetas o dispositivos físicos similares, que son utilizados para autenticación o almacenamiento de información financiera u otra información sensitiva, tomando en consideración las instalaciones relacionadas, dispositivos, empleados y métodos de validación utilizados.

3.2.3.6 Identificación y asignación de costos

Este objetivo satisface los requerimientos de negocio de asegurar un conocimiento correcto de los costos atribuibles a los servicios de Tecnología de Información.

Se hace posible a través de un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos, y toma en consideración:

- Los recursos identificables y medibles
- Los procedimientos y políticas de cargo
- Las tarifas

Tabla XXV. **Criterios y recursos en la identificación y asignación de costos**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	Confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
	P					P		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Elementos sujetos a cargo

La gerencia de la función de servicios de información deberá asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los usuarios. Los usuarios deberán ser capaces de controlar el uso de los servicios de información y de los niveles de facturación asociados.

b) Procedimientos de costeo

La gerencia de la función de servicios de información deberá definir e implementar procedimientos de costeo para proporcionar información gerencial acerca del costo de prestar servicios de información, asegurando al mismo tiempo la economía.

Las variaciones entre los costos pronosticados y los reales deberán ser analizadas adecuadamente y reportados, con el fin de facilitar el monitoreo de los mismos. Además, la alta gerencia deberá evaluar periódicamente los resultados de los procedimientos de contabilidad de costos de la función de servicios de información, a la luz de los otros sistemas de medición financiera de la organización.

c) Procedimientos de cargo y facturación a usuarios

La gerencia de la función de servicios de información deberá definir y utilizar procedimientos de cargo y facturación. Esta deberá mantener procedimientos de cargo y facturación que fomenten el uso apropiado de los

recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades. El monto cargado deberá reflejar los costos asociados con la prestación de servicios.

3.2.3.7 Capacitación de usuarios

El objetivo que satisface los requerimientos de negocio de asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.

Se hace posible a través de un plan completo de entrenamiento y desarrollo, y toma en consideración:

- El currículum de entrenamiento
- Las campañas de concientización
- Las técnicas de concientización

Tabla XXVI. **Criterios y recursos para la capacitación de usuarios**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	S							¤				

Objetivos de control detallados

a) Identificación de necesidades de entrenamiento

En línea con el plan a largo plazo, la gerencia deberá establecer y mantener procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información. Deberá establecerse un currículum de entrenamiento para cada grupo de empleados.

b) Organización del entrenamiento

Tomando como base las necesidades identificadas, la gerencia deberá definir los grupos objetivo, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.

Asimismo, deberán investigarse las opciones de entrenamiento (Localidad interna o externa, entrenadores internos o externos, etc.).

c) Entrenamiento sobre principios y conciencia de seguridad

Todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas. La alta gerencia deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de la función de servicios de información, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.

3.2.3.8 Apoyo y asistencia a los cliente de TI

Satisface los requerimientos de negocio de asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente, se hace posible a través de una oficina de ayuda que proporcione soporte y asesoría de primera línea, y toma en consideración:

- Las consultas de usuarios y respuesta a problemas
- El monitoreo de consultas y despacho
- El análisis y reporte de tendencias

Tabla XXVII. **Criterios y recursos para el apoyo y asistencia**

	Criterios de información							Recursos de TI				
	Efectividad	eficiencia	confidencialidad	Integridad	disponibilidad	Cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P									¤	¤			

Objetivos de control detallados

a) Oficina de ayuda

Deberá establecerse un soporte para usuarios dentro de una función de oficina de ayuda. Las personas responsables de llevar a cabo esta función deberán interactuar estrechamente con el personal de manejo de problemas.

b) Registro de preguntas del usuario

Deberán establecerse procedimientos para asegurar que todas las preguntas de los clientes sean registradas adecuadamente por la oficina de ayuda.

c) Escalamiento de preguntas del cliente

Los procedimientos de la oficina de ayuda deberán asegurar que las preguntas de los clientes, que no puedan ser resueltas inmediatamente, sean reasignadas apropiadamente dentro de la función de servicios de información, hasta el nivel adecuado para atenderlas.

d) Monitoreo de atención a clientes

La gerencia deberá establecer procedimientos para monitorear oportunamente la atención a las preguntas de los clientes. Las preguntas, que permanezcan pendientes por largo tiempo, deberán ser investigadas y atendidas.

e) Análisis y reporte de tendencias

Deberán establecerse procedimientos que aseguren el reporte adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias. Los reportes deberán ser analizados y sus resultados deberán ser atendidos adecuadamente.

3.2.3.9 Administración de configuración

El objetivo principal que satisface los requerimientos de negocio de dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios.

Se hace posible a través de controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

Y toma en consideración:

- El registro de activos
- La administración de cambios en la configuración
- El chequeo de *software* no autorizado
- Los controles de almacenamiento de *software*

Tabla XXVIII. **Criterios y recursos para la administración de configuración**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	Tecnología	instalaciones	datos
P				S		S			¤	¤	¤	

Objetivos de control detallados

a) Registro de la configuración

Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, en el momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo).

El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

b) Configuración base

La gerencia de la función de servicios de información deberá asegurarse de que exista una configuración base de elementos como punto de verificación, al cual regresar después de las modificaciones.

c) Registro de estatus

La gerencia de la función de servicios de información deberá asegurar que los registros de configuración reflejen el estatus real de todos los elementos de la configuración, incluyendo la historia de los cambios.

d) Control de la configuración

Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de la función de servicios de información sean revisadas periódicamente.

e) *Software* no autorizado

La gerencia de la función de servicios de información deberá revisar periódicamente la existencia de *software* no autorizado en las computadoras personales de la organización.

f) Almacenamiento de *software*

Deberá definirse un área de almacenamiento de archivos (biblioteca) para todos los elementos de *software* válidos en las fases apropiadas del ciclo de vida de desarrollo de sistemas. Estas áreas deberán estar separadas unas de otras y de las áreas de almacenamiento de archivos de desarrollo, pruebas y producción.

3.2.3.10 Administración de problemas e incidentes

El objetivo que satisface los requerimientos de negocio de asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir cualquier recurrencia.

Se hace posible a través de un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, y toma en consideración:

- Las suficientes pistas de auditoría de problemas y soluciones
- La resolución oportuna de problemas reportados
- Los procedimientos de escalamiento
- Los reportes de incidentes

Tabla XXIX. **Criterios y recursos para la administración de problemas**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P			S				¤	¤	¤	¤	¤

Objetivos de control detallados

a) Sistema de administración de problemas

La gerencia de la función de servicios de información deberá definir e implementar un sistema de administración de problemas, para asegurar que todos los eventos operacionales que no formen parte de la operación estándar (incidentes, problemas y errores) sean registrados, analizados y resueltos oportunamente. Deberán emitirse reportes de incidentes en el caso de problemas significativos.

b) Escalamiento de problemas

La gerencia deberá definir e implementar procedimientos de escalamiento de problemas, para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el procedimiento de escalamiento para la activación del plan de continuidad de tecnología de información.

c) Seguimiento de problemas y pistas de auditoría

El sistema de administración de problemas deberá proporcionar elementos adecuados para pistas de auditoría, que permitan el seguimiento de las causas a partir de un incidente (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

3.2.3.11 Administración de datos

Los objetivos que satisface los requerimientos de negocio de asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento.

Se hace posible a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI.

Además, toma en consideración:

- El diseño de formatos
- Los controles de documentos fuente
- Los controles de entrada
- Los controles de procesamiento
- Los controles de salida
- La identificación, movimiento y administración de la librería de medios
- La administración de almacenamiento y respaldo de medios
- La autenticación e integridad

Tabla XXX. **Criterios y recursos para la administración de datos**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
			P			P						¤

Objetivos de control detallados

1) Procedimientos de preparación de datos

La gerencia deberá establecer procedimientos de preparación de datos que va a ser seguidos por los departamentos usuarios. En este contexto, el diseño de formas de entrada de datos deberá ayudar a minimizar los errores y las omisiones.

Durante la creación de los datos, los procedimientos de manejo de errores deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

2) Procedimientos de autorización de documentos fuente

La gerencia deberá asegurar que los documentos fuente sean preparados apropiadamente por personal autorizado que actúa dentro de su autoridad, y que se establezca una separación de funciones adecuada respecto al origen y aprobación de documentos fuente.

3) Recopilación de datos de documentos fuente

Los procedimientos de la organización deberán asegurar que todos los documentos fuente autorizados estén completos, sean precisos, estén registrados apropiadamente y transmitidos oportunamente para la entrada de datos.

4) Manejo de errores de documentos fuente

Los procedimientos de manejo de errores durante la creación de datos deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

5) Retención de documentos fuente

Deberán establecerse procedimientos para asegurar que la organización pueda retener o reproducir los documentos fuente originales

durante un período de tiempo razonable para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requerimientos legales.

6) Procedimientos de autorización de entrada de datos

La organización deberá establecer procedimientos apropiados, para asegurar que la entrada de datos sea llevada a cabo únicamente por personal autorizado.

7) Chequeos de exactitud, suficiencia y autorización

Los datos sobre transacciones, capturados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.

8) Manejo de errores en la entrada de datos

La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.

9) Integridad de procesamiento de datos

La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de

actualización adecuados como totales de control "corrida a corrida", y controles de actualización de archivos maestros.

10) Validación y edición de procesamiento de datos

La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible.

Cuando se utilicen sistemas de inteligencia artificial, dichos sistemas serán ubicados en una infraestructura de control interactiva con operadores humanos, para asegurar que las decisiones vitales son aprobadas.

11) Manejo de errores en el procesamiento de datos

La organización deberá establecer procedimientos de manejo de errores en el procesamiento de datos, que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.

12) Manejo y retención de datos de salida

La organización deberá establecer procedimientos para el manejo y la retención de datos de salida de sus programas de aplicación de tecnología de información.

En caso de que instrumentos negociables (Ej. tarjetas de valor) sean los receptores de la salida, se deberá poner cuidado especial en prevenir usos inadecuados.

13) Distribución de datos de salida

La organización deberá establecer y comunicar procedimientos escritos para la distribución de datos de salida de tecnología de información.

14) Balanceo y conciliación de datos de salida

La organización deberá establecer procedimientos para asegurar que los datos de salida sean balanceados rutinariamente con los totales de control relevantes. Deberán existir pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de los datos con problema.

15) evisión de datos de salida y manejo de errores

La gerencia de la organización deberá establecer procedimientos para asegurar que la precisión de los reportes de los datos de salida sea revisada por el proveedor y por los usuarios relevantes. Asimismo, deberán establecerse procedimientos para controlar los errores contenidos en los datos de salida.

16) Provisiones de seguridad para reportes de salida

La organización deberá establecer procedimientos para garantizar que la seguridad de los reportes de datos de salida sea mantenida para todos

aquellos reportes que estén por distribuirse, así como para todos aquellos que ya hayan sido distribuidos a los usuarios.

17) Protección de información sensible durante transmisión y transporte

La gerencia deberá asegurar que, durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

18) Protección de información crítica por ser desechada

La gerencia deberá definir e implementar procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos deberán garantizar que ninguna información marcada como “borrada” o “desechada”, pueda ser accedida por personas internas o externas a la organización.

19) Administración de almacenamiento

Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requerimientos de recuperación, de economía y las políticas de seguridad.

20) Períodos de retención y términos de almacenamiento

Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de

entrada y de salida), así como los datos (claves, certificados) utilizados para su encriptamiento y autenticación.

21) Sistema de administración de la librería de medios

La función de servicios de información deberá establecer procedimientos para asegurar que el contenido de su librería de medios sea inventariado sistemáticamente, que cualquier discrepancia revelada por un inventario físico sea solucionada oportunamente, y que se lleven a cabo las medidas necesarias para mantener la integridad de los medios magnéticos almacenados en la librería.

22) Responsabilidades de la administración de la librería de medios

La gerencia de la función de servicios de información deberá establecer procedimientos de administración, para proteger el contenido de la librería de medios. Deberán definirse estándares para la identificación externa de medios magnéticos y el control de su movimiento y almacenamiento físico para soportar su seguimiento y registro. Las responsabilidades sobre el manejo de las librerías de medios (cintas magnéticas, cartuchos, discos y disquetes) deberán ser asignadas a miembros específicos del personal de servicios de información.

23) Respaldo y restauración

La gerencia deberá implementar una estrategia apropiada de respaldo y restauración, para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación.

Se deberán establecer procedimientos, para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.

24) Funciones de respaldo

Deberán establecerse procedimientos, para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

25) Almacenamiento de respaldos

Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

26) Archivo

La gerencia deberá implementar una política y procedimientos, para asegurar que el archivo cumple con requerimientos legales y de negocio y que se encuentra debidamente protegido y registrado adecuadamente.

27) Protección de mensajes sensitivos

Respecto a la transmisión de datos a través de Internet u otra red pública, la gerencia deberá definir e implementar procedimientos y protocolos para ser utilizados para el aseguramiento de la integridad, confidencialidad y "no negación" de mensajes sensitivos.

28) Autenticación e integridad

Previamente a que alguna acción crítica sea tomada sobre información originada fuera de la Organización que se reciba vía teléfono, correo de voz, documentos (en papel), fax o correo electrónico, se deberá verificar adecuadamente la autenticidad e integridad de dicha información.

29) Integridad de transacciones electrónicas

Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, la Gerencia deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas, que sean sensitivas y críticas para la organización, para asegurar la integridad y autenticidad de:

- atomicidad (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan);
- consistencia (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial);
- aislamiento (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente);

- durabilidad (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir fallas de sistema)

30) Integridad continua de datos almacenados

La gerencia deberá asegurar que la integridad y lo adecuado de los datos mantenidos en archivos y otros medios (Ej. tarjetas electrónicas) se verifique periódicamente. Atención específica deberá darse a dispositivos de valor, archivos de referencia y archivos que contengan información privada.

3.2.3.12 Administración de instalaciones

El objetivo que satisface los requerimientos de negocio de proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas, se hace posible a través de la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado.

Y toma en consideración:

- El acceso a instalaciones
- La identificación del centro de cómputo
- La seguridad física
- La salud y seguridad del personal
- La protección contra amenazas ambientales

Tabla XXXI. **Criterios y recursos en la administración de instalaciones**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
			P	P							¤	

Objetivos de control detallados

a) Seguridad física

Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información, de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a tener dicho acceso.

b) Discreción de las instalaciones de tecnología de información

La gerencia de la función de servicios de información deberá asegurar que se lleve un bajo perfil o discreción y que la identificación física de las instalaciones relacionadas con sus operaciones de tecnología de información sea limitada.

c) Escolta de visitantes

Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean escoltadas por algún miembro de ese grupo, cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

d) Salud y seguridad del personal

Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones internacionales, nacionales, regionales, estatales y locales.

e) Protección contra factores ambientales

La gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

f) Suministro ininterrumpido de energía

La gerencia deberá evaluar regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía, para las aplicaciones críticas de tecnología de información, con el fin de asegurarse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.

3.2.3.13 Administración de operaciones

El siguiente objetivo general satisface los requerimientos de negocio de asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

Se hace posible a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades, y toma en consideración:

- El manual de procedimiento de operaciones
- La documentación de procedimientos de arranque
- La administración de servicios de red
- La calendarización de personal y cargas de trabajo
- El proceso de cambio de turno
- El registro de eventos de sistemas

Tabla XXXII. **Criterios y recursos en la administración de operaciones**

Criterios de información								Recursos de TI				
Efectividad	Eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	Datos
P	P		S	S				¤	¤		¤	¤

Objetivos de control detallados

a) Manual de procedimientos de operación e instrucciones

La función de servicios de información deberá establecer y documentar procedimientos estándar para las operaciones de tecnología de información (incluyendo operaciones de red).

Todas las soluciones y plataformas de tecnología de información establecidas deberán ser operadas, utilizando estos procedimientos, los cuales deberán ser revisados periódicamente para asegurar su efectividad y cumplimiento.

b) Documentación del proceso de inicio y de otras operaciones

La gerencia de la función de servicios de información deberá asegurar que el personal de operaciones esté adecuadamente familiarizado y se sienta seguro con las tareas del proceso de inicio y con otras operaciones al tenerlas documentadas, y cuando éstas sean probadas y ajustadas periódicamente, según se requiera.

c) Calendarización de trabajos

La gerencia de la función de servicios de información deberá asegurar que la calendarización continua de trabajos, procesos y tareas sea organizada en la secuencia más eficiente, maximizando el proceso y la utilización, con el fin de alcanzar los objetivos establecidos en los convenios de nivel de servicio. Las caledarizaciones iniciales, así como los cambios a estas caledarizaciones deberán ser autorizados apropiadamente.

d) Salidas de la calendarización de trabajos estándar

Deberán establecerse procedimientos para identificar, investigar y aprobar las salidas de calendarización de trabajos estándar.

e) Continuidad de procesamiento

Los procedimientos deberán requerir continuidad de procesamiento durante los cambios de turno de operadores, mediante la existencia de un paso o entrega formal de actividades, actualizaciones y reportes de estatus sobre las responsabilidades actuales.

f) Bitácoras de operación

Los controles de la gerencia deberán garantizar que se esté almacenando suficiente información cronológica en bitácoras de operaciones, para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que lo rodean y soportan.

g) Operaciones remotas

Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la(s) instalación(es) remota(s) sean identificadas e implementadas.

3.2.4 Monitoreo

3.2.4.1 Monitoreo del proceso

Es el objetivo que satisface los requerimientos de negocio de asegurar el logro de los objetivos establecidos para los procesos de TI, se hace posible a través de la definición por parte de la gerencia de reportes e indicadores de desempeño gerenciales, la implementación de sistemas de soporte, así como la atención regular a los reportes emitidos, y toma en consideración:

- Los indicadores clave de desempeño
- Los factores críticos de éxito
- La evaluación de la satisfacción de clientes
- Los reportes gerenciales

Tabla XXXIII. **Criterios y recursos de monitoreo del proceso**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	S	S	S	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Recolección de datos de monitoreo

Para los procesos de tecnología de información y de control interno, la gerencia deberá asegurar que se definan indicadores de desempeño relevantes (Ej. comparaciones externas), tanto para actividades internas, como las proporcionadas por terceros y que se recolecten datos para la creación de reportes relevantes de desempeño y reportes de excepción relacionados con estos indicadores.

b) Evaluación de desempeño

Los servicios que van a ser proporcionados por la función de servicios de información deberán ser medidos (indicadores clave de desempeño y/o factores críticos de éxito) y comparados con los niveles objetivo. Las evaluaciones a la función de servicios de información deberán ser desarrolladas en forma continua.

c) Evaluación de la satisfacción de clientes

A intervalos regulares, la gerencia deberá efectuar mediciones de la satisfacción de los clientes respecto a los servicios proporcionados por la función de servicios de información, con la intención de identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento.

d) Reportes gerenciales

Deberán proporcionarse reportes gerenciales para ser revisados por la alta gerencia en cuanto al avance de la organización hacia las metas identificadas. Con base en la revisión, la Gerencia deberá iniciar y controlar las acciones pertinentes.

3.2.4.2 Evaluar lo adecuado de control interno

Satisface los requerimientos de negocio de asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

Se hace posible a través de el compromiso de la gerencia de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular, y toma en consideración:

- El monitoreo permanente de control interno
- La comparación con mejores prácticas
- Los reportes de errores y excepciones
- Las auto evaluaciones
- Los reportes gerenciales

Tabla XXXIV. **Criterios y recursos para la evaluación del control interno**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P	S	S	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Monitoreo de control interno

La gerencia deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones, a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

b) Operación oportuna de controles internos

La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la gerencia.

c) Reporte sobre el nivel de control interno

La gerencia deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas, para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

d) Seguridad de operación y aseguramiento de control interno

La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos, a través de una "auto auditoría" o de una auditoría independiente, para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos.

Las actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

3.2.4.3 Obtención de aseguramiento independiente

Satisface los requerimientos de negocio de incrementar los niveles de confianza entre la organización, clientes y proveedores externos.

Se hace posible a través de revisiones de aseguramiento independientes llevadas al cabo en intervalos regulares, y toma en consideración:

- Las certificaciones / acreditaciones independientes
- Las evaluaciones independientes de efectividad
- El aseguramiento independiente sobre cumplimiento de requerimientos legales y regulatorios
- El aseguramiento independiente de cumplimiento de compromisos contractuales
- Las revisiones a proveedores externos de servicios
- El aseguramiento de desempeño por personal calificado
- El involucramiento proactivo de auditoría

Tabla XXXV. **Criterios y recursos en la obtención de aseguramiento**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	Confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P	S	S	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Certificación / acreditación independiente de control y seguridad de los servicios de TI

La gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno, antes de implementar nuevos servicios de tecnología de información que resulten críticos y obtener recertificaciones o reacreditaciones de estas actividades en forma cíclica rutinaria después de haber hecho la implementación.

b) Certificación / acreditación independiente de control y seguridad de proveedores externos de servicios

La gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno, antes de utilizar proveedores de servicios de tecnología de información y obtener recertificaciones o reacreditaciones de estas actividades en forma cíclica rutinaria.

c) Evaluación independiente de la efectividad de los servicios de TI

La gerencia deberá obtener una evaluación independiente sobre la efectividad de los servicios de tecnología de información en forma cíclica rutinaria.

d) Evaluación independiente de la efectividad de proveedores externos de servicios

La gerencia deberá obtener una evaluación independiente sobre la efectividad de los proveedores de servicios de tecnología de información en forma cíclica rutinaria.

e) Aseguramiento independiente del cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales

La gerencia deberá obtener un aseguramiento independiente sobre el cumplimiento de la función de servicios de tecnología de información, respecto a requerimientos regulatorios y compromisos contractuales en forma cíclica rutinaria.

f) Aseguramiento independiente del cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales de proveedores externos de servicios

La gerencia deberá obtener un aseguramiento independiente sobre el cumplimiento de proveedores externos de servicios de tecnología de información, respecto a requerimientos regulatorios y compromisos contractuales en forma cíclica rutinaria.

g) Competencia de la función de aseguramiento independiente

La gerencia deberá asegurarse de que la función de aseguramiento independiente posee competencia técnica, habilidades y conocimiento necesario para desempeñar dicha función en una forma efectiva, eficiente y económica.

h) Participación proactiva de auditoría

La gerencia de tecnología de información deberá buscar la participación de auditoría en una forma proactiva, antes de finalizar soluciones de servicio de tecnología de información.

3.2.4.4 Proveer auditoría independiente

Satisface los requerimientos de negocio de incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas, se hace posible a través de auditorías independientes desarrolladas en intervalos regulares, y toma en consideración:

- La independencia de auditoría
- El involucramiento proactivo de auditoría
- La ejecución de auditorías por parte de personal calificado
- La aclaración de resultados y recomendaciones
- Las actividades de seguimiento

Tabla XXXVI. **Criterios y recursos para la auditoria independiente**

Criterios de información								Recursos de TI				
Efectividad	eficiencia	confidencialidad	integridad	disponibilidad	cumplimiento	confiabilidad		recursos	aplicación	tecnología	instalaciones	datos
P	P	S	S	S	S	S		¤	¤	¤	¤	¤

Objetivos de control detallados

a) Estatutos de auditoría

La alta gerencia de la organización deberá establecer los estatutos para la función de auditoría. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoría. Asimismo este documento deberá ser revisado periódicamente, para asegurar que se mantengan la independencia, autoridad y responsabilidad de la función de auditoría.

b) Independencia

El auditor deberá ser independiente del auditado, tanto en actitud como en apariencia (real y percibida). Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa. De esta manera, la función de auditoría deberá ser suficientemente independiente del área auditada, para concluir una auditoría en forma objetiva.

c) Ética y estándares profesionales

La función de auditoría deberá asegurar el cumplimiento de los códigos aplicables de ética profesional (Ej. Código de Ética de la *Information Systems Audit and Control Association*) y estándares de auditoría (Ej. Estándares de la *Information Systems Audit and Control Association*) en todo lo que lleve a cabo.

El debido cuidado profesional, deberá observarse en todos los aspectos del trabajo de auditoría, incluyendo el respeto de estándares aplicables sobre auditoría y tecnología de información.

d) Competencia

La gerencia deberá asegurar que los auditores responsables de las revisiones de las actividades de la función de servicios de información de la organización, sean técnicamente competentes y cuentan en forma general con las habilidades y conocimientos (Ej. dominios de CISA) necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica. La gerencia deberá asegurar que el personal asignado a tareas de auditoría de sistemas de información, mantiene su nivel de competencia técnica mediante un programa adecuado de educación profesional continua.

e) Planeación

La alta gerencia deberá establecer un plan de auditoría para garantizar que se obtenga un aseguramiento regular e independiente, respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno, así como de la habilidad de la gerencia para controlar las actividades de la función de servicios de información. Dentro de este plan, la gerencia deberá determinar las prioridades relacionadas con la obtención de aseguramiento independiente. Los auditores deberán planear el trabajo de auditoría para alcanzar los objetivos de auditoría y cumplir con los estándares profesionales correspondientes.

f) Ejecución del trabajo de auditoría

Las auditorías deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoría están siendo alcanzados y que los estándares profesionales de auditoría que sean aplicables están siendo observados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil, para alcanzar los objetivos de auditoría de forma efectiva. Los hallazgos y conclusiones de auditoría deben estar soportadas por un análisis apropiado y una correcta interpretación de esta evidencia.

g) Reporte

La función de auditoría de la organización deberá proporcionar un reporte en un formato adecuado, para todo el personal interesado una vez concluida su revisión. El reporte de auditoría deberá mostrar los objetivos de la auditoría, el período de cobertura y la naturaleza y extensión de trabajo de auditoría realizado. El reporte deberá identificar a la organización, los destinatarios del informe y cualquier restricción en su circulación. El reporte de auditoría deberá también mostrar los hallazgos, conclusiones y recomendaciones relacionadas con el trabajo de auditoría lleva do acabo, así como cualquier salvedad o comentario que el auditor tenga respecto a la auditoría.

h) Actividades de seguimiento

La resolución acerca de los comentarios sobre la auditoría depende de la gerencia. Los auditores deberán solicitar y evaluar información pertinente sobre hallazgos, conclusiones y recomendaciones previos, para determinar si las acciones apropiadas han sido implementadas de manera oportuna.

4. APLICACIÓN DE LOS OBJETIVOS DE CONTROL EN ADQUISICIÓN E IMPLEMENTACIÓN

4.1 Descripción del problema

4.1.1 Descripción general de la empresa

El caso de aplicación que se desarrolla en el presente trabajo, está basado en una empresa real, la cual se dedica en su parte medular a la compra y venta de productos. Actualmente no cuenta con ninguna área de producción, puesta en marcha, ni existen planes para ello.

Constituye a la organización una cadena de tiendas distribuidas a nivel nacional, las cuales se abastecen desde una bodega central, que también realiza operaciones de ventas por medio de vendedores con territorios predefinidos. La empresa está formada por las gerencias que se mencionan a continuación: ventas, compras, financiera, informática, logística y recursos humanos, además de la gerencia general o administrativa.

La empresa dentro del área administrativa se divide en departamentos que dependen de las gerencias antes mencionadas, los cuales se pueden clasificar de la siguiente manera:

- Compras
- Ventas
    - Punto de venta
    - Locales

    - Telefónicas
- Bodega
    - Bodega central
    - Bodegas sucursales
    - Destrucción
- Contabilidad
- Tesorería – bancos –
- Recursos humanos
    - Planilla
    - Selección
    - Capacitación
- Presupuestos
- Costos
- Auditoría
- Cuentas por cobrar – créditos –
- Cuentas por pagar

La empresa se dedica específicamente a la compra y venta de productos, los cuales dependiendo de la generación de una necesidad, que es iniciada por varios factores, se realiza una orden de compra a un proveedor específico, el cual después de su verificación y obtención de dicha orden, despacha la mercadería solicitada.

Esta mercadería llega a bodega central para ser ingresada, tanto al inventario físico, como al inventario de sistema, y después de una revisión es llevada a estanterías para su posterior distribución.

El área de ventas en la cadena de sucursales es abastecida desde bodega central, después de que la información de sus ventas de un día anterior es cargada y procesada

dentro del sistema y por lo tanto se generan solicitudes de pedido de manera automática, los cuales se preparan y distribuyen a cada una de las sucursales. Ésta llega a sucursales, en donde es preparada y colocada para su venta a clientes externos.

Dentro de esta misma área, se encuentran las ventas desde bodega central para clientes terceros, las cuales generan un pedido hacia un cliente específico y con un vendedor determinado, y son ingresadas a solicitud de cada uno de los vendedores.

Los departamentos antes mencionados generan sendas solicitudes al departamento de bodega, el cual se encarga de recoger, preparar, chequear y colocar los productos para su respectiva distribución, ya sea local o clientes terceros. Si son clientes terceros, las existencias solamente afectan a bodega central, en cambio, si es a sucursales de la cadena, entonces se debe de afectar los dos inventarios para poder llevar un control como espejo de las existencias en sucursales.

Existen también dentro de la estructura organizacional los departamentos de Contabilidad, Tesorería, Cuentas por cobrar y Cuentas por pagar, los cuales interactúan con los antes ya mencionados para se fusionen y formen parte de su complemento en las diversas actividades que realizan. Es decir, que la contabilidad es el centro de todos ellos, ya que aquí se registran las transacciones contables de lo que cada uno de los anteriores realiza. Y entre ellos se genera información que uno ingresa y otro procesa, según el nivel de relación que exista dentro de los procesos definidos en la empresa.

Se cuenta, dentro de los departamentos de la empresa, uno que se encarga de la realizar auditorías en todo nivel, ya sea a nivel de conteo de productos y realización de inventarios en las sucursales, como también en el desarrollo de seguimiento de papeles y cuadres importantes para la organización.

En las sucursales se llevan a cabo distintos procesos, como son la recepción de mercadería, la colocación de la misma, así como la venta a clientes finales, para posteriormente ejecutar un corte de las operaciones realizadas dentro de la caja. Posteriormente a esto, se ejecuta un cierre de operaciones que es el que se toma en cuenta para el proceso de envío de información a la central y con esto se cuenta con los datos necesarios para poder llevar las cuenta de qué, cómo, cuánto, cuándo y en dónde se están vendiendo actualmente los productos.

Se cuenta con una ficha técnica que maneja la información del producto, así como sus descuentos, la forma de resurtir el inventario de las sucursales, que es con base en máximos y mínimos, aunque siempre se ha evaluado la posibilidad de realizar las solicitudes de pedido por reposición de ventas del día anterior; esto es para poder llevar mantener el surtido completo en la sucursal. La empresa cuenta con ventas por medio de vendedores a clientes externos, los cuales deben hacer su pedido, el cual se ingresa en las oficinas centrales y se procesa como una solicitud normal.

Otra de las áreas importantes de la empresa es la venta a domicilio, para lo cual se tiene un lugar, en el cual se centralizan las comunicaciones telefónicas de los clientes y se toman los pedidos, como si fueran atendidos desde una de las sucursales que pertenecen a la cadena.

La empresa cuenta actualmente con dos sistemas de información, los cuales procesan la información dependiendo del modulo en el cual se encuentren; el desarrollo de las aplicaciones nuevas se está realizando en casa, para lo cual se necesita hacer un diagnostico por medio de una herramienta evaluativo para saber la forma de cómo se está realizando el desarrollo, y la implementación de *software* en la empresa.

El sistema anterior se desarrolló en una herramienta carácter, mientras que el desarrollo nuevo se está desarrollando en un ambiente gráfico; existe intercambio de información en las dos vías, del sistema anterior al sistema nuevo y viceversa.

4.1.2 Área específica a estudiar – adquisición e implementación –

En el departamento de sistemas de información de la empresa, se cuenta con un área específicamente dedicada al desarrollo e implementación de programas y utilitarios necesarios para facilitar el funcionamiento de las operaciones que en estas se generan. El objetivo principal de este análisis es poder tener de una manera cuantitativa y objetiva de evaluar el funcionamiento y la estrategia que se ha llevado a cabo dentro del campo de la tecnología de información y especialmente en el área de adquisición e implementación de sistemas.

El recurso humando está conformado dentro del área de desarrollo e implementación por 3 personas, con un conocimiento a nivel medio – avanzado, un perfil de estudios profesionales terminado, conocimiento de las herramientas que va a ser utilizadas y una experiencia de varios años programación sobre el lenguaje utilizado.

Las aplicaciones en la empresa se han implementado, según la solicitud e importancia que la gerencia le dé a los módulos que se necesitan; en el caso a estudiar, se decidió empezar por el modulo de general.

Todos los módulos están desarrollados en un ambiente grafico, con utilización de herramientas 4GL que dan apoyo en el desarrollo de soluciones. Se dividen en tres áreas de desarrollo el de formas, reportes y el de procedimientos en base de datos.

En sí la definición del problema va a estar limitada a todos aquellos procesos y procedimientos que, dentro de la gerencia de tecnología de información, aseguren un claro análisis de las adquisiciones e implementaciones, utilizando todas las oportunidades y mediante un mejor enfoque que pueda cumplir con los requerimientos por parte de los usuarios, en el cual se involucren diversos factores como estudios de factibilidad, costo – beneficio, instalaciones y auditoría, que es el modelo que se utiliza para la ingeniería de *software* entre otros.

Se deben de definir e identificar las soluciones de tecnología de información, ya sea desarrolladas o adquiridas y no olvidar que dentro de los temas de estudio se debe de incluir los cambios y el mantenimiento, que permita realizar el *software* y sistemas existentes.

Un punto a tocar, dentro del análisis del tema, es el de la adquisición de *software*, el cual debe de proporcionar funciones que soporte efectivamente el negocio, en la cual se tomen en cuenta los requerimientos de diversos usuarios, pruebas y documentación. Otro de los más importantes, dentro de la organización, es la correcta adquisición y posterior implementación de la arquitectura de *software* y contar con las plataformas apropiadas, para soportar los cambios del medio y las aplicaciones de negocios.

Otro tema de consideración para la adquisición e implementación sería el de desarrollo y mantenimiento de procedimientos relacionados con tecnología de información, el cual asegura el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Con esto se asegura que las instalaciones de *software* lleven el respectivo entrenamiento y distintos conjuntos de pruebas, y se deja por último la administración de cambios, para poder minimizar la cantidad de interrupciones no autorizadas y errores.

4.2 Metodología

La metodología utilizada, en el área de adquisición e implementación, está orientada utilizando el marco metodológico del COBIT (Control Objectives for information and related Technology), el cual es una herramienta ampliamente aceptada por la comunidad internacional de auditores de sistemas de información como una norma estándar.

4.2.1 Breve Introducción de COBIT

La Misión de COBIT es "Investigar, desarrollar, publicar y promover un conjunto de objetivos de controlen tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores." (ISACAF-EXS, 2000).

COBIT está diseñado como un estándar aplicable y aceptable en general para la buena práctica de la auditoría de las tecnologías de la Información en todo el mundo. El producto COBIT utiliza los objetivos de control de ISACA, mejorados con estándares específicos de tipo técnico, profesional, normativo e industrial existentes y emergentes. Los objetivos de control se han desarrollado para su aplicación en el amplio espectro de sistemas de información en la empresa.

El sistema consiste en objetivos de control de TI de alto nivel y una estructura global para su clasificación y funcionamiento. La teoría subyacente para la clasificación elegida, en línea con las experiencias de reingeniería es que hay, en esencia, tres niveles de esfuerzos en TI, cuando se considera la gestión de los recursos de TI:

- **Actividades**: las actividades, junto con las tareas, están en el nivel inferior. Las actividades tienen el concepto de ciclo de vida, mientras que las tareas se consideran discretas en el tiempo.
- **Procesos**: se definen en un nivel superior como series de actividades unidas con puntos de control naturales.
- **Dominios**: corresponden al nivel superior, son agrupaciones de procesos. COBIT distingue cuatro dominios en línea con el ciclo de gestión o el ciclo de vida, que son aplicables a los procesos de TI; los dominios se dividen en cuatro grandes categorías que son:
    - Planeación y organización
    - **Adquisición e implementación**
    - Distribución y soporte
    - Monitoreo

El marco conceptual se enfoca desde tres puntos de vista distintos: criterios de gestión para la información, recursos de TI y procesos de TI. Estos tres puntos de vista se ensamblan en un formato cúbico y permiten que se obtengan referencias cruzadas en dicho marco, y se pueda acceder a él eficientemente.

No todas las medidas de control satisfarán los requisitos de gestión en el mismo grado, así que se hace una distinción en COBIT, contemplando el cumplimiento:

- **Primario** (**P**): es el grado en que el objetivo de control satisface completamente el requisito de información correspondiente.
- **Secundario** (**S**): es el grado en que el objetivo de control satisface solamente en menor extensión o indirectamente el requisito de información correspondiente

4.2.2 Adquisición e implementación

Es el área que pertenece a COBIT que se encarga de llevar a cabo la estrategia de tecnología de información, en la cual las soluciones de TI deben de ser identificadas, ya sea desarrolladas o adquiridas, para que posteriormente se implementen y puedan integrarse a los procesos del negocio. Además, dentro de este dominio, se cubren los cambios y el mantenimiento realizados a los sistemas existentes.

Este dominio se subdivide en seis objetivos generales, los cuales se desglosan a su vez en específicos, y se mencionan a continuación:

- Identificación de soluciones:
    - Definición de requerimientos de información
    - Estudios de factibilidad
    - Arquitectura de Información
    - Pistas de auditoría
    - Contratación de terceros
    - Aceptación de instalaciones y tecnología

- Adquisición y mantenimiento de *software*
    - Requerimientos de usuarios
    - Requerimientos de archivo, entrada, proceso y salida
    - Interfase usuario – máquina
    - Personalización de paquetes
    - Pruebas funcionales
    - Controles de aplicación y requerimientos funcionales
    - Documentación

- Adquisición y mantenimiento de arquitectura de tecnología
    - Evaluación de tecnología

- Mantenimiento preventivo de *hardware*
- Seguridad del *software* de sistema, instalación, mantenimiento y control sobre cambios

- Desarrollo y mantenimiento de procedimientos relacionados con tecnología de información
  - Procedimientos y controles de usuarios
  - Procedimientos y controles operacionales
  - Materiales de entrenamiento

- Instalación y acreditación de sistemas
  - Capacitación
  - Conversión / carga de datos
  - Pruebas específicas
  - Acreditación
  - Revisiones post implementación

- Administración de cambios.
  - Identificación de cambios
  - Procedimientos de categorización, priorización y emergencia
  - Evaluación del impacto
  - Autorización de cambios
  - Manejo de liberación
  - Distribución de *software*

4.3 Solución

El análisis del área de Adquisición e Implementación se llevó a cabo por medio del estudio de los objetivos de control detallado, que se exponen en la metodología

COBIT. Estos, a su vez, se desglosaron en un conjunto de preguntas por objetivo específico, que da como resultado un cuestionario de diagnóstico del área en estudio.

Por otra parte, se definen los elementos que toman parte de cada uno de los objetivos generales y se realiza una matriz de estudio de responsabilidades y elementos afectados en cada uno de los objetivos generales. Esto es la funcionalidad de determinar los elementos que forman parte del estudio y la parte en la que pueden colaboran, según el proceso que se esté realizando.

4.3.1 Identificación de soluciones

Se comienza el estudio por la Identificación de soluciones, en la cual los recursos de TI que se utilizan son: sistemas de aplicación, tecnología e instalaciones, y los criterios de información que se van tomar en cuenta son la efectividad y eficiencia.

A continuación, se presenta el detalle de la matriz que muestra la relación que tienen los elementos con los objetivos de control detallados:

Tabla XXXVII. **Relación de elementos con los objetivos de control**

Elementos	Requerimiento de información	Acciones alternativas	Estrategias de adquisición	Servicios de terceros	Factibilidad tecnológica	Factibilidad económica	Arquitectura de información	Análisis de riesgos	Controles de seguridad	Pistas de auditoría	Ergonomía	Selección de software	Control de abastecimiento	Adquisición de producto sw.	Mantenimiento de sw. tercero	Programación de aplicaciones	Aceptación de instalaciones	Aceptación de tecnología
Alta gerencia				¤					¤					¤				
Gerencia informática	¤	¤	¤	¤	¤	¤	¤		¤		¤	¤	¤		¤		¤	¤
Gerencia de operaciones				¤														
Técnicos sistemas										¤	¤							
Técnicos tecnología																		
Administrador de sistemas	¤	¤				¤	¤	¤		¤	¤	¤	¤		¤	¤		¤
Administrador de tecnología					¤	¤							¤		¤			¤
Usuario final																¤		
Tecnologías					¤													
Proveedores de hw.					¤													
Proveedores de sw																¤		¤
Metodología de ciclo de vida	¤	¤	¤															¤
Hw. de servidores	¤																	
Hw. de redes	¤																	
Sw. de s. operativo	¤	¤													¤	¤		
Sw. Base de datos	¤	¤													¤	¤		
Sw. Aplicaciones	¤	¤									¤				¤	¤		
Sw. Utilitarios	¤	¤													¤	¤		

Se enumeran los elementos que forman parte de la adquisición e implementación de *software* en la empresa, en la cual se realiza el estudio; estos elementos pueden tomar participación en cualquier momento y con cualquier objetivo de control.

Es por eso que se establece la relación de los mismos, mediante la utilización de una matriz de referencia cruzada, en la cual se demuestra de manera gráfica quién tiene responsabilidades en cada objetivo de control que se va a estudiar y analizar.

Como se puede observar, para cada uno de los objetivos de control, puede existir más de un colaborador, ya que cada objetivo general se divide en varios objetivos específicos que buscan cumplir una tarea, para la realización exitosa de los objetivos generales.

En la tabla siguiente, se muestra un cuadro de diagnóstico elaborado para la alta gerencia de sistemas, que ayude a empezar a indagar qué es lo qué sucede con los sistemas de información, dentro de este caso en estudio.

Se presentan los resultados de la encuesta realizada al jefe de sistemas de la empresa en estudio, los cuales son tabulados para poder establecer posteriormente las conclusiones y las recomendaciones, lo cual busca de una manera objetiva, no subjetiva, cuál es el efecto actual de la adquisición e implementación de los sistemas de información de la empresa.

Tabla XXXVIII **Cuestionario de diagnóstico para la identificación de soluciones**

Cuestionario de diagnóstico
Identificación de soluciones
Empresa <Nombre de empresa>

A continuación, se muestran una serie de preguntas, las cuales se deben de responder de forma directa, y ordenada.

#	Pregunta
1	Dentro del ciclo de vida del software de la empresa, tanto para la adquisición como para el desarrollo, ¿existen requerimientos definidos en las siguientes áreas (Si / No)?

Software	Sí
Datos	Sí
Infraestructura	Sí

2 Para cada una de las áreas de la pregunta anterior, defina si se incluyen los siguientes aspectos dentro de sus soluciones funcionales:

	Software	Datos	Infraestructura
Desempeño	X		
Protección	X	X	x
Confiabilidad	X	x	x
Compatibilida	X	x	

d

Seguridad X x

Legislación X

3 ¿La metodología del ciclo de vida formula soluciones alternativas, que satisfagan los requerimientos del negocio?

Sí x No

¿Cual de las siguientes estrategias de adquisición de software se

4 utiliza actualmente?

Software terminado

Desarrollo interno

Combinación de

anteriores

5 ¿Existe un formato o solicitud de propuesta y un procedimiento de evaluación para servicios de terceros?

Sí X No

6 ¿ Se realiza un estudio de factibilidad tecnológica por alternativa de solución?

Sí x No

7 ¿Se realiza un estudio de factibilidad económica y análisis de costos, en cada proyecto de desarrollo?

Sí x No

8 Además, ¿se realiza un análisis de beneficios asociados?

Sí x No

9 ¿Se examina el modelo de datos de la empresa para definir las soluciones y analizar la factibilidad de las mismas?

Sí No x

¿Existe un reporte del análisis de riesgos por cada proyecto, que

10 cuente con?

	Análisis y documentación de amenazas	No
	Estudios de puntos de impacto	No
	Debilidades existentes	No

¿Se definen los costos y beneficios en términos monetarios de los mismos?

11

	Sí	x	No

¿Dentro del procedimiento de aprobación se cuenta con la firma de la alta gerencia?

12

	Sí	x	No

¿Se cuenta con mecanismos adecuados para contar con pistas de auditoría?

13

	Sí	x	No

14 ¿ Los procesos de desarrollo, implementación y cambios son ergonómicos?

	Sí	No	x

15 ¿La organización cuenta con un procedimiento estándar para identificar los programas de software que satisfagan los requerimientos operacionales?

	Sí	No	x

16 ¿ Existe dentro de la empresa un procedimiento y estándares en la adquisición de?

Hardware	No
Software	No
Servicios	No

17 ¿Los productos son revisados y probados previo a su pago?

	Sí	No	X

18 ¿Se cuenta con políticas de adquisición de software?

	Sí	No	X

19 ¿Se revisan los procedimientos de los proveedores de *software* con los cuales validan, protegen y mantienen los derechos de integridad sus productos?

	Sí	x	No

20 En el contrato de programación de software, ¿se cuenta con una justificación de Servicio?

	Sí	No	x

21 ¿El *software* y la documentación adquirida estan sujeto a pruebas?

	Sí	x	No

22 Marque con una 'x' los tipos pruebas que se tiene estipulado en un contrato de productos de software:

Sistema	X	Proced.	x	Regresión	
Integración	X	Carga	x	Aceptación de usuario	x
Hardware	X	Estrés		Piloto de sistema	x

23 Cuando se acepta una instalación, marque a un lado, lo que se encuentra definido:

Procedimientos	x
Criterios	x
Pruebas	x

24 Para la aceptación de tecnología, ¿existe un contrato entre el

proveedor y gerencia?

Sí X No

4.3.1.1 Comentarios

De esto, se puede concluir que el objetivo de identificación de soluciones se está trabajando de manera objetiva, tomando en cuenta las directrices y objetivos de la empresa; su actuación esta de acuerdo con las necesidades y visión de la organización; faltan algunos puntos que no son críticos y se cumple con un gran porcentaje de los puntos evaluados.

4.3.2 Adquisición y mantenimiento de aplicación

De la misma manera que se estudió el primer objetivo general, a continuación se examina el de adquisición y mantenimiento de *software* aplicativo, en donde el único recurso de tecnología de información que se toca es el de sistemas de aplicación y los factores críticos son, como primarios la eficiencia y la efectividad y como secundarios la integridad, el cumplimento y la confiabilidad.

Las relaciones que existen entre los elementos y los objetivos de control, para poder realizar la adquisición y el mantenimiento de una aplicación de *software*, se muestran en la siguiente tabla:

Tabla XXXIX. **Relación entre los elementos y los objetivos de control para la adquisición y mantenimiento de la aplicación**

Elementos	Métodos de diseño	Cambios significativos a sistemas	Aprobación del diseño	Def. Y doc. de req. de archivos	Especificaciones de prog.	Recopilación de datos fuente	Def. Y doc. De req. De entrada	Definición de interfases	Interfases usuario-máquina	Def. Y doc. de req. de procesamiento	Def. Y doc. de req. de salida	Controlabilidad	Disponibilidad	Estipulación de integridad	Pruebas de sw. de aplicación	Materiales de consulta	Reevaluación de diseño
Alta gerencia			¤														
Gerencia informática		¤	¤		¤	¤				¤	¤			¤		¤	¤
Gerencia de operaciones			¤											¤			¤
Técnicos sistemas	¤	¤	¤	¤	¤	¤	¤	¤	¤			¤	¤		¤	¤	
Técnicos tecnología								¤							¤	¤	
Administrador de sistemas	¤	¤	¤	¤	¤			¤		¤	¤			¤			¤
Administrador de tecnología								¤						¤			¤
Usuario final	¤		¤						¤							¤	
Tecnologías																	
Proveedores de hw.																	
Proveedores de sw																	
Metodología de ciclo de vida	¤	¤	¤	¤	¤	¤	¤	¤	¤		¤		¤				
Hw. de servidores																	
Hw. de redes																	
Sw. de s. operativo																	
Sw. base de datos				¤				¤									
Sw. aplicaciones								¤									
Sw. utilitarios																	

En esta matriz de referencia cruzada, entre los elementos que intervienen y los objetivos de control para la adquisición y mantenimiento de la aplicación, se muestran las relaciones que se lograron identificar en la empresa estudiada y del análisis de las mismas se deriva, el cuestionario de diagnóstico para la evaluación y la correcta aplicación de los métodos de la adquisición, así como el mantenimiento. El cuestionario se muestra a continuación:

Tabla XXXX **Cuestionario de diagnóstico para la adquisición y mantenimiento del *software* de aplicación**

Cuestionario de diagnóstico

Adquisición y mantenimiento de software de aplicación

Empresa <Nombre de empresa>

A continuación, se muestra una serie de preguntas, las cuales se deben de responder de forma directa, y ordenada.

#	Pregunta	
1	Respecto al método del ciclo de vida de desarrollo de sistemas, se puede preguntar lo siguiente:	
	¿Las técnicas y los procedimientos son los apropiados?	No
	¿Existe la relación entre usuarios y creación de las especificaciones del programa?	Si
	¿Se verifica Diseño vrs. Requerimientos?	No
2	¿Se lleva el mismo proceso de desarrollo con los cambios significativos de cada una de las aplicaciones?	
	Sí	X
	No	
3	Marque con una X por quien es aprobado y revisado el diseño para cada proyecto	
	Alta gerencia	
	Gerencia	x
	Usuarios	x
	Todos	
4	¿Existe un procedimiento para la definición de cada proyecto y la documentación de los formatos de los archivos?	
	Sí	
	No	x

5 Si existe, ¿respeta las reglas del diccionario de datos?

	Sí	No	x

6 ¿Se prepara por escrito la especificación de programa?

	Sí	No	x

7 ¿Existe correspondencia entre la especificación del programa y el diseño de datos?

	Sí	X	No

8 ¿Se cuenta con la especificación del mecanismo para recopilar la entrada de datos?

	Sí	No	x

9 ¿Existen los mecanismos para definir y documentar los requerimientos?

	Sí	No	x

10 Marque con una x, si existe, los siguientes elementos para las interfases Interna y Externa

	Interno	Externo
Especificación		x
Diseño	X	x
Documentación		x

11 La interfase usuario - máquina es de fácil utilización

	Sí	x	No

12 Esta interfase , ¿cuenta con auto documentación de ayuda en línea?

	Sí	No	x

13 ¿Existe la definición de requerimientos de procesamiento y modificaciones?

	Sí		No	x

14 ¿Se documentan todos los requerimientos?

	Sí		No	x

15 ¿Se definen las salidas de datos y los procesos que las motivan?

	Sí		No	x

16 ¿Se documentan de alguna manera las salidas que genera el sistema?

	Sí		No	x

17 ¿En qué nivel, el programa incluye controles de aplicación que garantice que los datos de entrada y salida estén correctos?

Alto	
Medio	x
Bajo	
Ninguno	

18 ¿Se verifican las siguiente características en los datos de entrada y salida?

		autorizació	
precisión	x	n	x
Oportunida			
d	x		

19 ¿Se evalúa la seguridad y control dentro del sistema?

	Sí		No	x

20 ¿La disponibilidad está considerada en el proceso desde el diseño?

	Sí		No	x

21 ¿Aplica que los programas verifiquen rutinariamente las tareas realizadas por el *software*?

	Sí		No	x

22 ¿Existe el procedimiento de recuperación de datos en

reserva?

Sí	No	x	

23 ¿Se aplican las siguientes pruebas al software?

Unitarias	X	De carga	x
De aplicación	X	Estrés	x
De integración	X		

24 Dentro de la organización, ¿se cuenta con un estándar de pruebas?

Sí	No	x

25 ¿Existe para las aplicaciones un manual de referencia y soporte?

Sí	x	No

26 ¿Se reevalúa el software periódicamente?

Sí	No	x

4.3.2.1 Comentarios

Dentro de lo que se puede concluir, a partir del estudio que se realiza en la empresa, se puede recomendar que dadas las circunstancias, se debe de aplicar una ingeniería de software, empezando por definir un método de análisis y diseño, y buscar mayor apoyo en cada una de las fases.

Se deben de fortalecer las pruebas y mantener el orden mientras se desarrolla, separar las áreas de desarrollo y mantenimiento dentro, debido a que causa conflictos a nivel de utilización de orden. Las pruebas se realizan de manera subjetiva por parte del desarrollador.

Por último, se recomienda invertir más tiempo en la documentación de los sistemas, ya sea a nivel interno o externo, hasta el nivel del usuario.

4.3.3 Adquisición y mantenimiento de arquitectura de TI

La adquisición y mantenimiento de la arquitectura de tecnología de información no permite evaluar el desempeño de las dos grandes áreas. El recurso por parte de tecnología de información es la tecnología, y sus criterios de información son efectividad, eficiencia e integridad.

Las relaciones que se encontraron entre sus elementos que se describen mediante una tabla de referencia cruzada, entre los objetivos de control y sus elementos.

En esta matriz, se descubren de manera detallada las relaciones que existen entro los elementos, que intervienen en la adquisición y mantenimiento de la arquitectura de TI y los objetivos de control que son aplicables al mismo.

Tabla XXXXI **Relación entre los elementos y los objetivos de control para la adquisición y mantenimiento de arquitectura de TI**

Elementos	Sw.	Mantenimiento preventivo	Seguridad de sw. del sistema	Instalación del sw de sistema	sistema	Controles para cambios de sw
Alta gerencia						
Gerencia informática	¤	¤	¤	¤	¤	¤
Gerencia de operaciones						
Técnicos sistemas					¤	¤
Técnicos tecnología	¤	¤	¤			
Administrador de sistemas				¤	¤	¤
Administrador de tecnología	¤	¤	¤			
Usuario final						
Tecnologías						
Proveedores de hw.		¤				
Proveedores de sw						
Metodología de ciclo de vida						
Hw. de servidores		¤				
Hw. de redes		¤				
Sw. utilitarios			¤	¤	¤	

El cuestionario de diagnóstico de cómo se maneja el área de adquisición y mantenimiento de la arquitectura del *software* muestra algunos resultados interesantes, como por ejemplo las áreas en que deben mostrarse más atención, debido a que se establece un comportamiento correctivo, en lugar de ser preventivo.

Este cuestionario se deriva del estudio de la metodología del COBIT y de los objetivos, que se deben de cumplir para su correcta aplicación, implementación y adquisición de soluciones en la arquitectura de tecnología.

Tabla XXXXII **Cuestionario de diagnóstico en la adquisición y mantenimiento de la arquitectura de *software***

Cuestionario de diagnóstico
Adquisición y mantenimiento de arquitectura de software
Empresa <Nombre de empresa>

1 ¿Existe un procedimiento de evaluación del estado en el que se encuentra el Hardware de la Organización?

Sí No x

2 ¿Existe un procedimiento dentro de la empresa para la evaluación de *software*?

Sí No x

3 ¿Están calendarizados para toda la organización los mantenimientos preventivos?

Sí No x

4 ¿Con qué periodicidad se dan los mantenimientos a los equipos de computación?

Mucha

Media

Poca

Correctiva x

5 ¿Las instalaciones de software arriesgan la seguridad de los datos y los programas ya almacenados?

Sí No x

6 ¿Se siguen las instrucciones recibidas por los expertos de producto, para su correcta instalación e implementación?

Sí No x

7 ¿Se realizan pruebas suficientes y necesarias para asegurar el funcionamiento, antes de entrar en producción?

Sí No x

8 ¿Existe la figura, dentro de los servicios de información, de mantenimiento de *software*?

Sí No x

9 ¿Las modificaciones se hacen de manera controlada y de acuerdo con una política de administración de cambios?

Sí No x

4.3.3.1 Comentarios

Lo que nos indica el resultado del cuestionario de diagnosis es que se debe de ordenar la evaluación de *hardware y software*, ya que aunque se haga de una manera actualmente, es conveniente tener normados este tipo de eventos.

Además, se puede observar la parte de mantenimiento a los equipos de *hardware* es primordial, debido a que se pueden reducir costos de manejo, transporte y envío, de equipo que puede mantenerse mas tiempo en uso, si se le diera el trato adecuado, Por último, se debe de realizar todos los cambios y mantenimientos de *software*, que depende de las recomendaciones de los proveedores, se deben de seguir sus pasos y si se puede documentarlos.

4.3.4 Desarrollo y mantenimiento de procedimientos de TI

El desarrollo y mantenimiento de procedimientos de tecnología de información es uno de los puntos administrativos y teóricos más importantes, por que desde aquí se realiza el control a nivel procedural de muchas de los factores que afectan el TI.

Éste cuenta para su realización los siguientes recursos de TI: recursos, sistemas de aplicación, tecnología, instalaciones; los siguientes criterios de información: de manera primaria: efectividad, eficiencia, y secundario: integridad, cumplimiento y confiabilidad.

Este punto se lleva a cabo mediante un enfoque totalmente estructurado del desarrollo de manuales de procedimientos para los usuarios, requerimientos de servicio y material de entrenamiento.

Los objetivos de control tienen una orientación hacia la documentación total, para el uso de los usuarios y de los procedimientos, que estos deben de realizar para poder llevar a cabo sus tareas de manera correcta y, a la vez, alimentar la información con datos útiles para el uso de toda la corporación.

Los cuadros de relación se muestran en la siguiente tabla:

Tabla XXXXIII. **Relación de los elementos y los objetivos para el desarrollo y mantenimiento de los procesos de TI**

Elementos	Futuros requerimientos	procedimientos	Manual de operación	entrenamiento
Alta gerencia				
Gerencia informática	¤	¤	¤	¤
Gerencia de operaciones				
Técnicos sistemas		¤	¤	¤
Técnicos tecnología		¤	¤	¤
Administrador de sistemas	¤	¤	¤	¤
Administrador de tecnología	¤	¤	¤	¤
Usuario final		¤		¤
Tecnologías				
Proveedores de hw.				
Proveedores de sw				
Metodología de ciclo de vida	¤	¤	¤	¤
Hw. de servidores				
Hw. de redes				
Sw. Utilitarios				

A partir del análisis de la tabla de relaciones que existen entre los elementos y los objetivos de control, se puede desprender que la responsabilidad, en su gran mayoría, cae sobre los mandos de mayor rango dentro de la organización, lo que indica que en este punto se requiere mucha dirección de los mandos altos y mandos medios, para poder definir de forma correcta cuáles serán los pasos para poder implementar de manera procedural, lo procesos involucrados, que a la vez se unen con los sistemas de información. El cuestionario de diagnóstico para esta área es el que se presenta a continuación:

Tabla XXXXIV. **Cuestionario de diagnóstico en el desarrollo y mantenimiento de los procedimientos de TI**

Cuestionario de diagnóstico

Desarrollo y mantenimiento de procedimientos de TI

Empresa <Nombre de empresa>

1	¿Existe una definición oportuna de requerimientos operacionales, dentro de la metodología aplicada en el ciclo de vida del *software*?		
	Sí	No	x
2	¿Se toman en cuenta dentro de la metodología aplicada los servicios futuros?		
	Sí	No	x
3	¿Existen manuales de procedimiento para los usuarios?		
	Sí	No	x
4	¿La corporación cuenta con un manual de operaciones adecuado y actualizado?		
	Sí	No	x
5	¿Existe material de entrenamiento, práctico y adecuado en que se enfoque al uso del sistema de información en la práctica diaria?		
	Sí	No	x

4.3.4.1 Comentarios

Es importante tomar en cuenta a estos controles y procedimientos, ya que regulan y ordenan los procedimientos y procesos existentes dentro de una organización; se recomienda poner en marcha un plan de acción que permita la creación de estas

herramientas, que son útiles a los usuarios finales, y por consiguiente, descargan un poco del trabajo a las áreas de sistemas y tecnología.

4.3.5 Instalación y acreditación de sistemas

En la Instalación y acreditación de sistemas, se verifica y se confirma que la solución sea adecuada para el propósito deseado. Esto se hace por medio de todos los recursos de la tecnología de información, que son: recursos, sistemas de aplicación, tecnología, instalaciones y datos; tanto los criterios de información, efectividad, como el primario; como secundarios, están integridad y disponibilidad. Entonces, el cuadro de relaciones sería el siguiente:

Tabla XXXXV. **Relación de los elementos y los objetivos de control para la instalación y acreditación de sistemas**

Elementos	Entrenamiento	Adecuación	Conversión	Pruebas de cambios	Pruebas piloto	Pruebas de aceptación	Pruebas y acreditación	Prueba operacional	Promoción a producción	Evaluación de satisfacción	Revisión post-	
Alta gerencia						¤	¤		¤			
Gerencia informática	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	¤	
Gerencia de operaciones	¤				¤	¤	¤		¤			
Técnicos sistemas	¤	¤	¤	¤		¤				¤	¤	
Técnicos tecnología			¤									
Administrador de sistemas	¤	¤	¤	¤	¤	¤				¤	¤	
Administrador de tecnología			¤		¤							
Usuario final	¤	¤	¤	¤	¤	¤	¤	¤		¤	¤	
Tecnologías												
Proveedores de hw.												
Proveedores de sw												
Metodología de ciclo de vida			¤									
Hw. de servidores				¤								
Grupo de pruebas						¤	¤					
Hw. de redes												
Sw. Utilitarios	¤			¤	¤	¤						

El cuestionario de diagnóstico derivado de los objetivos de control que se van a cumplir se muestra a continuación, el cual tabula la información recopilada, dentro de estudio efectuado a la empresa en cuestión.

Cuestionario de diagnóstico

Instalación y acreditación de sistemas

Empresa <Nombre de empresa>

1 Dentro de la Organización, ¿existe un plan de entrenamiento o capacitación como parte de cualquier proyecto de desarrollo?

Sí No x

2 ¿Existe material relacionado como apoyo didáctico para las capacitaciones desarrolladas?

Sí x No

3 En los procedimientos del departamento de sistemas de información y su ciclo de vida, ¿existe uno de conversión de datos de un sistema anterior a un sistema nuevo?

Sí No x

4 ¿Existe dentro del departamento de sistemas un grupo de personas dedicadas a pruebas, que no sean los desarrolladores?

Sí No x

5 ¿Existe un ambiente de pruebas completo, que cuente como mínimo una instancia igual a la real, más los cambios solicitados?

Sí X No

6 Dentro del conjunto de pruebas, ¿se realizan evaluaciones de impacto y recursos?

Sí No x

7 ¿Existen desarrollados planes de respaldo externo?

Sí No x

8 ¿El ambiente de pruebas es representativo del operacional, es decir, que cuentan con condiciones similares de seguridad, controles internos, cargas de trabajo entre otros?

Sí x No

9 ¿Existe un plan para realizar pruebas piloto, que cuente con procedimientos previamente establecidos que aseguren su correcta implementación?

Sí No x

10 ¿Están definidos los criterios para terminar el proceso de pruebas y su aceptación final?

Sí No X

11 ¿Las pruebas cubren todas los componentes del sistema de información por lo menos en las áreas de *software* de aplicación, instalaciones, tecnología y procedimientos de usuarios?

Sí No x

12 ¿Existe una evaluación y aprobación formal por parte de la gerencia?

Sí x No

13 ¿Quiénes evalúan las pruebas de aceptación final de los sistemas de información adquiridos?

Operaciones

Usuarios x

Gerencia	x	
Todos		

14 Del grupo anterior, que es el encargado de evaluar las pruebas de aceptación, indique si evalúan los siguientes aspectos:

Nivel de Seguridad	No
Riesgo residual	No
Producto Completo	Si
Condiciones Similares	No

15 ¿Están claramente definidos los procedimientos para controlar las entregas de adquisiciones de *software*?

Sí		No	x

16 De los siguientes aspectos post-implementación, marque con una X los que se evalúan

Capacidad y desempeño	x	Costo	
Nivel de satisfacción	x	Beneficio	

4.3.5.1 Comentarios

Los resultados indican que en la organización, en la cual se aplica el estudio, a la parte de las pruebas no se le da la importancia que tiene, por lo que es necesario contar con un grupo especializado en probar las aplicaciones de *software*, que se tenga el tiempo que se necesita para realizar las pruebas, y a la vez definir conjuntos de trabajo responsables de ciertas tareas y criterios. Que puedan aceptar y dar por concluido el período de pruebas, así como definir los procesos y políticas que acompañen y rijan el funcionamiento de las pruebas en general.

4.3.6 Administración de cambios

En la administración de cambios, también se utilizan todos los recursos de tecnología de información, es decir, se utilizan los recursos, sistemas de aplicación, tecnología, infraestructura y datos. Los criterios de Información son primarios: efectividad, eficiencia, integridad, disponibilidad, y el secundario es la confiabilidad. La matriz de relaciones es la siguiente:

Tabla XXXXVI. **Relación de los elementos y los objetivos de control para la administración de cambios**

Elementos	Requisición de cambio	Evaluación de impacto	Control de cambios	Doc. y procedimientos	Mantenimiento	Liberación de sw	Distribución de sw	
Alta gerencia								
Gerencia informática	¤	¤	¤	¤	¤	¤	¤	
Gerencia de operaciones								
Técnicos sistemas		¤	¤	¤	¤			
Técnicos tecnología				¤				
Administrador de sistemas		¤	¤	¤	¤			
Administrador de tecnología				¤		¤	¤	
Usuario final	¤		¤					
Tecnologías							¤	
Proveedores de hw.								
Proveedores de sw								
Metodología de ciclo de vida								
Hw. de servidores								
Grupo de pruebas								
Hw. de redes								
Sw. utilitarios								

Derivado de los objetivos de control descritos en el capitulo tres y correspondientes a la administración de cambios, se puede extraer el siguiente cuestionario de diagnóstico, que cuenta como objetivo principal tabular y extraer la información de manera ordenada, para su posterior procesamiento y análisis. Éste se muestra en la siguiente tabla:

Tabla XXXXVII. **Cuestionario de diagnóstico en la administración de cambios**

Cuestionario de diagnóstico
Administración de cambios
Empresa <Nombre de empresa>

1	La requisición de cambio, tanto internos como externos, ¿tiene un estándar?			
		Sí	No	x
2	¿Existen procedimientos formales de administración de cambios?			
		Sí	No	x
3	Marque con una X, las propiedades que se encuentran identificadas en una solicitud de los cambios			
		Categorizada	Urgentes	x
		Priorizada	x	
4	¿Se evalúa en una forma estructurada el impacto que tiene o que puede tener el cambio?			
		Sí	x	No

5	¿Se documenta y se archiva cada uno de los cambios que se realizan?		
	Sí	No	x
6	En la parte de Mantenimiento , ¿se cumplen las siguientes restricciones?		
	Asignación especifica		x
	Monitoreo de trabajo		x
	Accesos controlados		x
7	¿Se cuentan con medidas de control específicas para asegurar la distribución del elemento de software?		
	Sí	X	No
8	Además, ¿cuenta con las pistas de auditoria necesarias para su seguimiento y desarrollo?		
	Sí	No	x

4.3.6.1 Comentarios

Los resultados obtenidos, en la administración de cambios, revelan que éste se maneja a un nivel superior que los anteriores; a excepción del primero, existe un mejor seguimiento de los cambios, que dejan mejores rastros. Al mismo tiempo se evalúan los impactos que los cambios pueden tener en determinado módulo y momento.

Es necesario poner en práctica la documentación y procedimientos que puedan dar una directriz genérica de cómo se debe de hacer, para que los cambios sean actualizados de la manera que corresponde.

CONCLUSIONES

1. La diferencia de concepto que existe entre la auditoría informática y la auditoría de sistemas de información radica en que esta nueva definición abarca la necesidad de controlar globalmente los sistemas de información, desde su planificación hasta su implementación, sin dejar por un lado las estrategias de la organización.

2. Existe la necesidad de encontrar la unión y el entendimiento entre la alta dirección gerencial y el departamento de tecnología de información, por medio de una metodología fácil, inductiva y eficaz, a nivel empresarial. Esto se logra a través de la metodología COBIT, que funciona como el enlace que busca explicar, de una manera gerencial, por medio de objetivos, los procesos y actividades que se dan dentro del departamento de TI.

3. El desarrollo de la metodología COBIT, dentro de una organización y la correcta aplicación y entendimiento de los objetivos de control, en cada uno de los dominios, es decir en la planificación y organización, adquisición e implementación, entrega de soporte y servicios y monitoreo, permite realizar un diagnóstico objetivo de cómo se encuentra la tecnología de información, cómo se manejan los procesos y cómo se aplican las soluciones dentro de la misma.

4. El dominio de la adquisición e implementación, por medio de los objetivos de control, permite evaluar e identificar las soluciones de *software* que más le conviene a una empresa; se muestra cuáles son los puntos y temas importantes que se deben considerar, así como la factibilidad de cada uno de los proyectos en el área de Tecnología y Económica. Se establecen los procedimientos para poder realizar una adquisición y la forma por medio de la cual se ejecutan. Para poder llevar a cabo un proyecto, se debe de examinar y evaluar la arquitectura de tecnología, tanto en *software* como en *hardware*. Por último dentro de los objetivos, se evalúa la forma y la estrategia con la cual se acreditan los sistemas de información.

5. El resultado obtenido por las encuestas realizadas a empresas guatemaltecas muestra que solamente el 18% de las mismas realizan algún tipo de auditoría de sistemas (ver figura 10, apéndice A), con lo cual muestra la poca importancia que sienten las empresas de nuestro medio a realizar estudios y utilizar metodologías que auditen los sistemas de información. Sin embargo, al segmentar la muestra y clasificarla en grandes, medianas y pequeñas los resultados obtenidos son los siguientes, para las empresas grandes el 24% realizan auditoría de sistemas (ver figura 4, apéndice A); en cambio en las empresas clasificadas como medianas, se observa que solamente un 10 % de las mismas la realiza (ver figura 6, apéndice A), y por último en las empresas pequeñas, se obtiene un resultado de 0 % de utilización en el uso de auditoría de los sistemas de información (ver figura 8, apéndice A).

RECOMENDACIONES

1. Se debe analizar la necesidad de la creación de un equipo, si no lo existiera, dentro de la organización, que se encargue de la evaluación de los sistemas de información, desde la planificación hasta el monitoreo del funcionamiento de las aplicaciones y procedimientos, que se utilizan en el departamento de TI, dividiendo y seccionando cada una de las áreas.

2. Hay que establecer el porcentaje de entendimiento con el que cuenta la alta dirección gerencial de los procesos, procedimientos y sistemas que se utilizan en el área de tecnología de información (Ver apéndice B), además de la importancia que significa la información en la toma de decisiones, para que, basado en los dos datos anteriores, se pueda evaluar la utilización de una metodología para el diagnostico de TI, como COBIT, que le permita tener una amplia y completa visión al equipo empresarial, de cómo se debe de invertir de una manera clara y objetiva en los sistemas de información.

3. En la adquisición e implementación de *software*, se debe de tomar en cuenta, la forma correcta y los pasos que conlleva la adquisición de *software*. Se deben de definir las fases con las cuales se va a realizar la implementación, así como la documentación necesaria que será entregada a cada uno de los proveedores, lo cual depende de las necesidades de la organización previamente establecidas; así también se debe definir una metodología clara a seguir para el desarrollo e implementación de *software*.

4. Es conveniente tomar en cuenta las directrices generalmente aceptadas de auditoría y desarrollar un conjunto de herramientas de implementación, que se basa en cada uno de los objetivos de control de la metodología COBIT, tanto en los objetivos de alto nivel, como en cada uno de los específicos. Se puede realizar, en forma de una encuesta de respuesta directa, para buscar la tabulación de resultados y su análisis de objetivo.

BIBLIOGRAFÍA

- Adkoli, Anand. **Manual de Oracle 8 para Windows NT**. España. McGraw-Hill/ Interamericana. 1999. 397pp.
- Alonzo Rivas, Gonzalo. **Auditoría Informática**. 2ª ed. España. Ediciones Díaz de Santos S.A. 1988. 185pp.
- Alta Dirección. **La auditoria en la era de la informática.** España. Ediciones Nauta. S.A. 1982. 163pp.
- CASIC. **Curso de Auditoría de Sistemas de Información Computarizada**. Guatemala. Centro de adiestramiento de personal. 1981. 115pp.
- Echenrique García, José Antonio. **Auditoria en Informática**. México. McGraw-Hill / Interamericana. 1990. 203pp.

- Loney Kevin. **Oracle 8 Manual del Administrador**. España. McGraw-Hill / Interamericana. 2000. 708pp.
- Muller Robert. **Manual de Oracle Developer/2000**. España. McGraw-Hill / Interamericana. 1998. 573pp.

- Piattini, Mario Gerardo y Emilio del Peso Navarro. **Auditoría Informática: un enfoque práctico.** 3ª ed. España. Editorial Alfa– Omega. 1998. 605pp.
- Rivas, Antonio de Juan y Aurora Pérez Pascual. **La auditoría en el desarrollo de proyectos informáticos.** 2ª ed. España. Ediciones Díaz de Santos S.A. 1988. 157pp.

- www.isaca.org Sitio del Information Systems Audit and Control Foundation

APÉNDICE A

- **Formato de cuestionario de diagnóstico:**

Cuestionario de diagnóstico
Utilización de la auditoría de sistemas en las empresas

Tesis "Los objetivos de Control en la Tecnología de Información (COBIT) y su aplicación con la auditoría de sistemas"

1. ¿Se realiza dentro de la empresa alguna auditoria de sistemas, para el área de tecnología de información?

   Sí ☐ No ☐

2. Si su respuesta es positiva en la pregunta anterior, ¿qué metodología utilizan para evaluar las distintas áreas de la auditoría de sistemas?

   _____

3. ¿Qué estándares de auditoría se utilizan dentro de su empresa?
   - COSO _____
   - SAC _____
   - SAS 55 y SAS 78 _____
   - COBIT _____
   - OTROS _____

4. En la evaluación de la auditoría de sistemas, ¿se evalúa el área de planeación y organización del departamento de TI?

Sí ☐ No ☐

Si su respuesta es positiva, marque con una "X" , los temas sobre los cuales se realiza:

Definición del plan estratégico de TI		Administración del recurso humano	
Definición de la arquitectura de información		Asegurar el cumplimiento de requerimientos	
Determinación de la dirección tecnológica		Evaluación de riesgos	
Definición de la organización y relaciones de TI		Administración de proyectos	
Manejo de la inversión de TI		Administración de calidad	
Comunicación de directrices gerenciales			

5. En la evaluación de la auditoría de sistemas, ¿se evalúa el área de adquisición e implementación dentro departamento de TI?

Sí ☐ No ☐

Si su respuesta es positiva, marque con una "X" , los temas sobre los cuales se realiza:

Identificación de soluciones		Desarrollo y manten. de procedimientos de ti	
Adquisición y manten. de software		Instalación y acreditación de sistemas	
Adquisición y manten. de arquitectura de ti		Administración de cambios	

6. En la evaluación de la auditoría de sistemas, ¿se evalúa el área de entrega de servicios y soporte dentro departamento de TI?

Sí ☐ No ☐

Si su respuesta es positiva, marque con una "X" los temas sobre los cuales se realiza:

Definición del nivel de servicio		Soporte a los clientes de TI	
Admón. del servicio de terceros		Admón. de la configuración	
Admón. de la capacidad y el desempeño		Admón. de problemas e incidentes	
Asegurar el servicio continuo		Admón. de datos	
Garantizar la seguridad del sistema		Admón. de instalaciones	
Identificación y asignación de costos		Admón. de Operaciones	
Capacitación de usuarios			

7. En la evaluación de la auditoría de sistemas, ¿se evalúa el área de monitoreo dentro departamento de TI?

Sí ☐ No ☐

Si su respuesta es positiva, marque con una "X" los temas sobre los cuales se realiza:

Seguimiento de procesos		Obtención de aseguramiento independiente	
Evaluación de lo adecuado del control interno		Proveer una auditoría independiente	

- **Resultados de cuestionario de diagnóstico en gráficas**

Las gráficas siguientes muestran los resultados obtenidos, a partir de las encuestas realizadas a diferentes empresas del medio guatemalteco. El tamaño de la muestra es de 50 empresas escogidas totalmente independientes y al azar, las cuales fueron clasificadas en tres categorías de la siguiente manera:

Clasificación	**Porcentaje**
Grandes	(68.00 %)
Medianas	(20.00 %)
Pequeñas	(12.00 %)
	(100.00 %)

Para poder clasificarlas en cada una de las categorías, se tomó en cuenta principalmente el tamaño físico de la empresa, es decir, por la cantidad de sucursales o por el tamaño de las instalaciones principales y por la cantidad de productos que éstas comercian, ya que algunas de ellas no cuentan con sucursales, pero pertenecen al grupo de empresas grandes.

De esta manera, se evaluaron en forma puntual los diferentes aspectos, en los cuales se aplica la metodología COBIT, y la auditoría de sistemas de información. Se mostraron primero las estadísticas de cada una de las clasificaciones en las que se segmentó el universo de empresas (grande, mediana y pequeña), y se dejó en la parte final del apéndice el resultado de las estadísticas de manera general (sin clasificación de empresas); se muestran en sus gráficas los resultados de la aplicación de cada uno de los objetivos de la metodología COBIT.

Resultados por categoría de empresa:

Figura 4. Resultado de auditoría de sistemas en empresas grandes

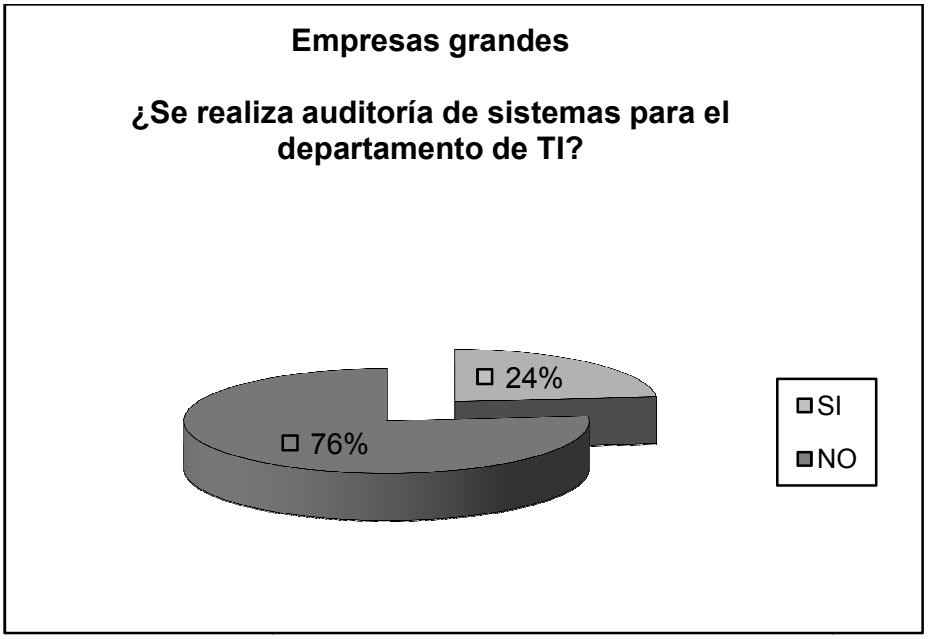


Figura 5. Principales áreas evaluadas en empresas grandes

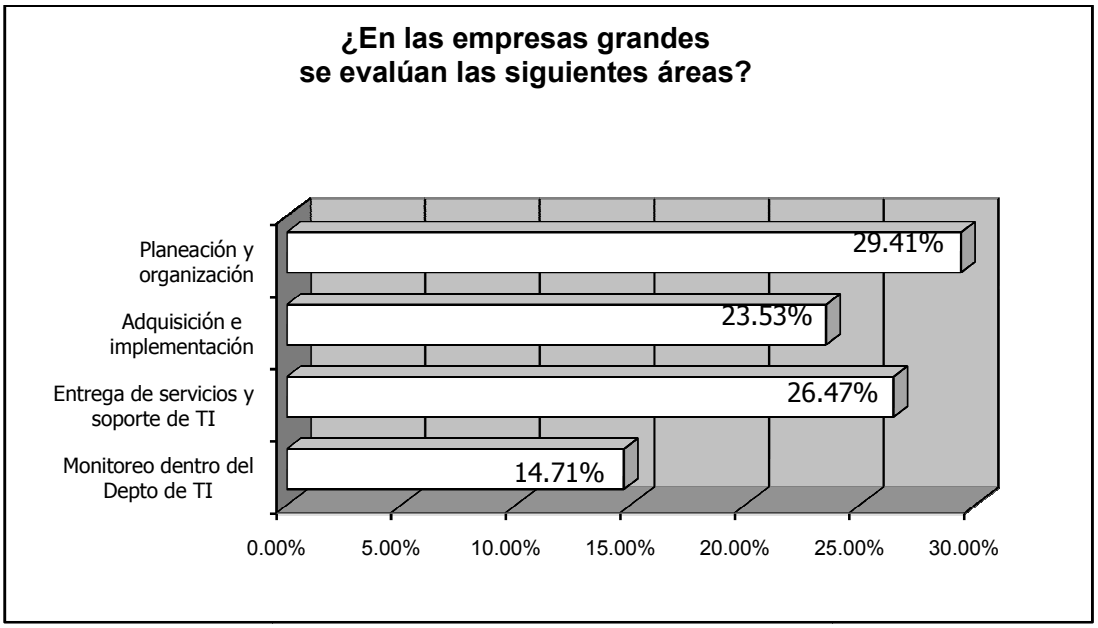


Figura 6. Resultado de auditoría de sistemas en empresas medianas

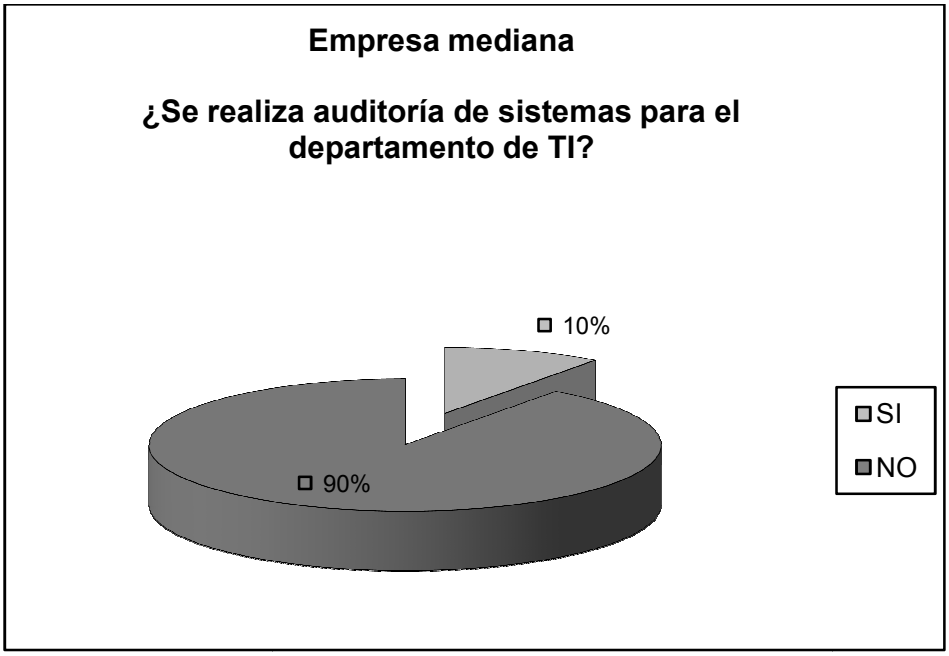


Figura 7. Principales áreas evaluadas en empresas medianas

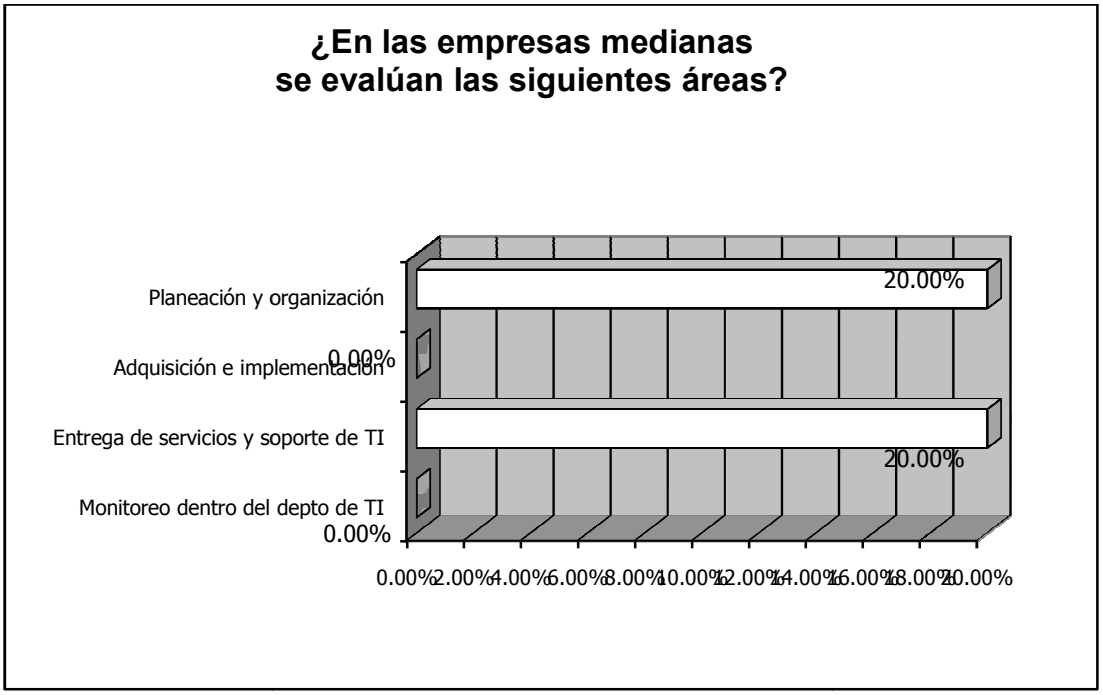


Figura 8. Resultado de auditoría de sistemas en empresas pequeñas

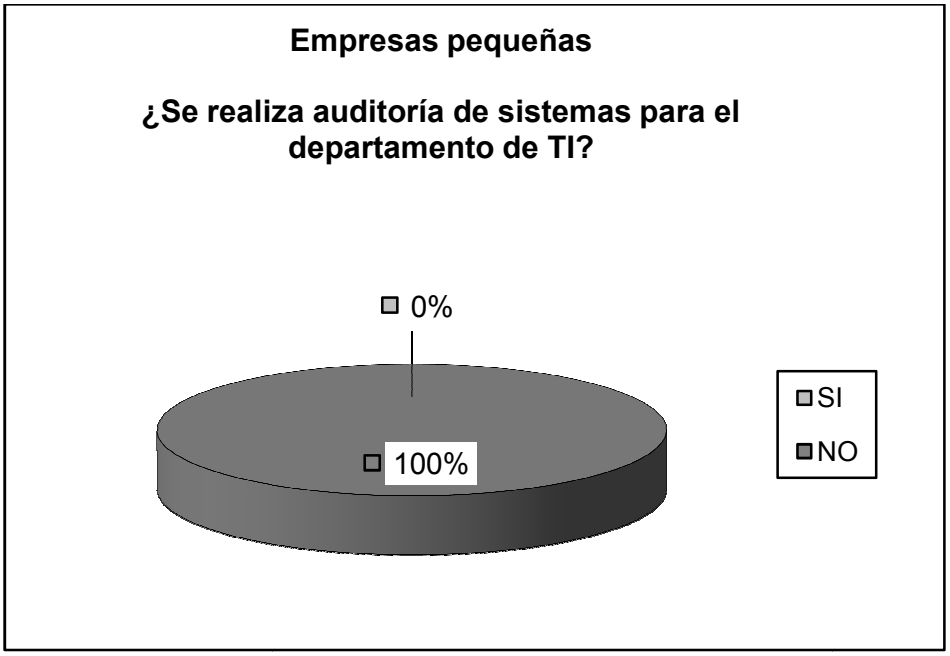
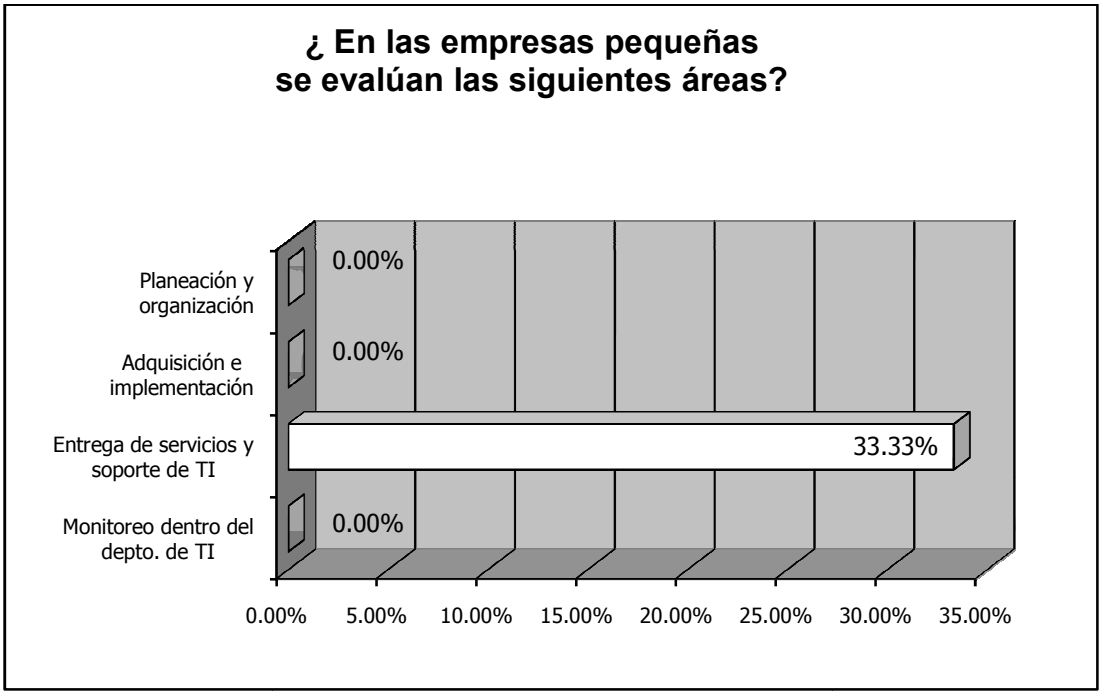


Figura 9. principales áreas evaluadas en empresas pequeñas



Resultados Totales (Sin Clasificación de Empresa)

Los resultados que se muestran a continuación son de la muestra total, sin tomar en cuenta las clasificaciones de las empresas; por eso los porcentajes en cada una de las categorías evaluadas cambia levemente de valor.

Figura 10. Resultado de auditoría de sistemas

Figura 11. Resultado porcentual del área de planeación y organización

Figura 12. Resultado porcentual del área de adquisición e implementación

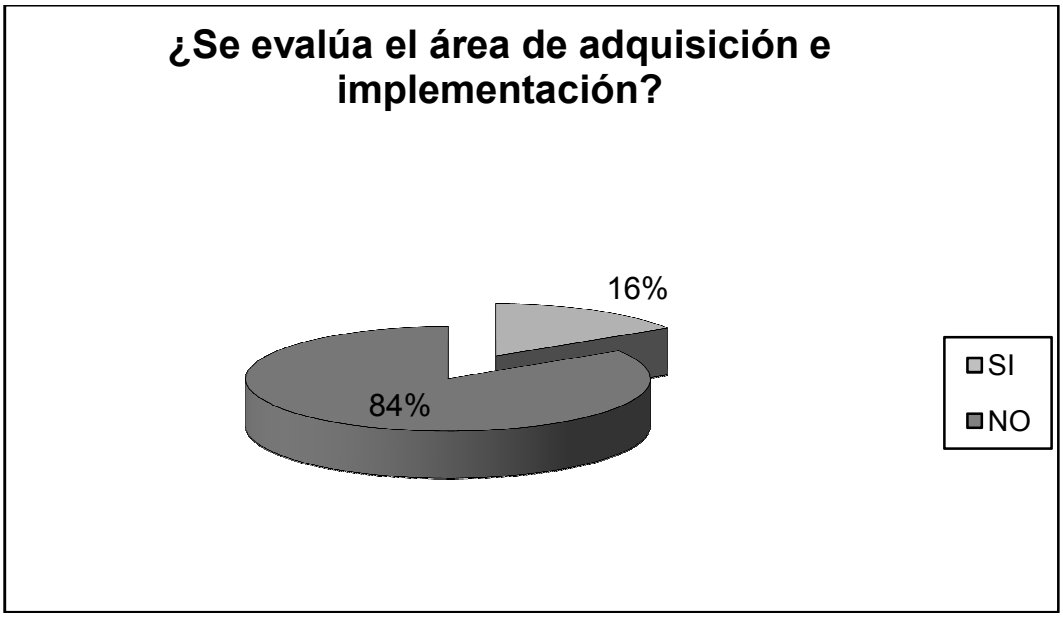


Figura 13. Resultado porcentual del área de entrega de servicios y soporte

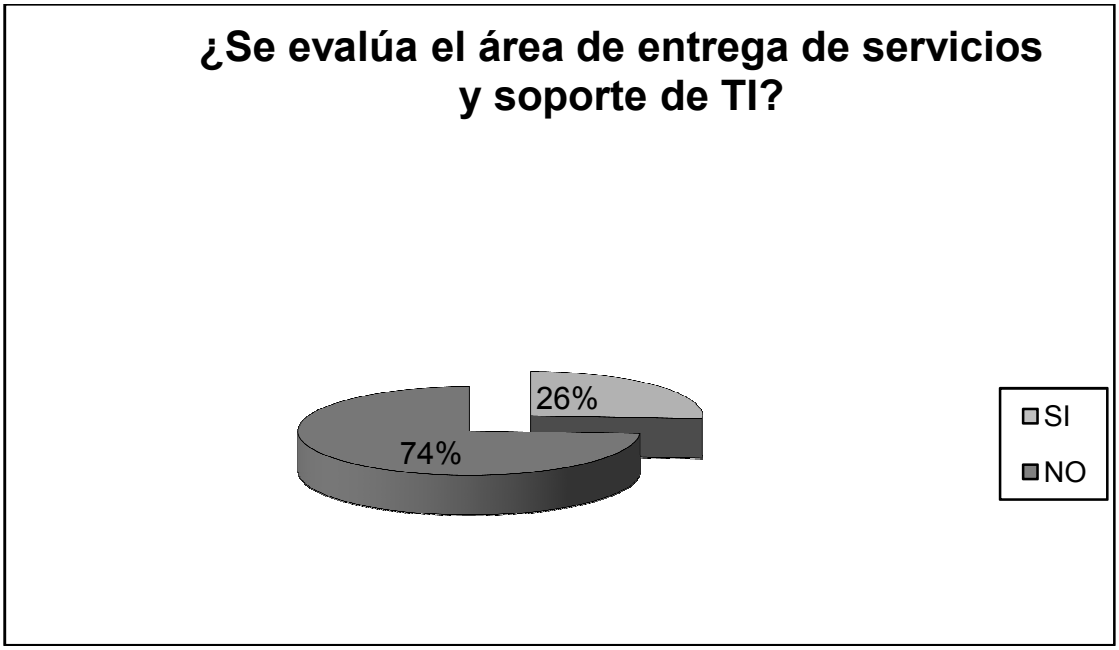


Figura 14. Resultado porcentual del monitoreo

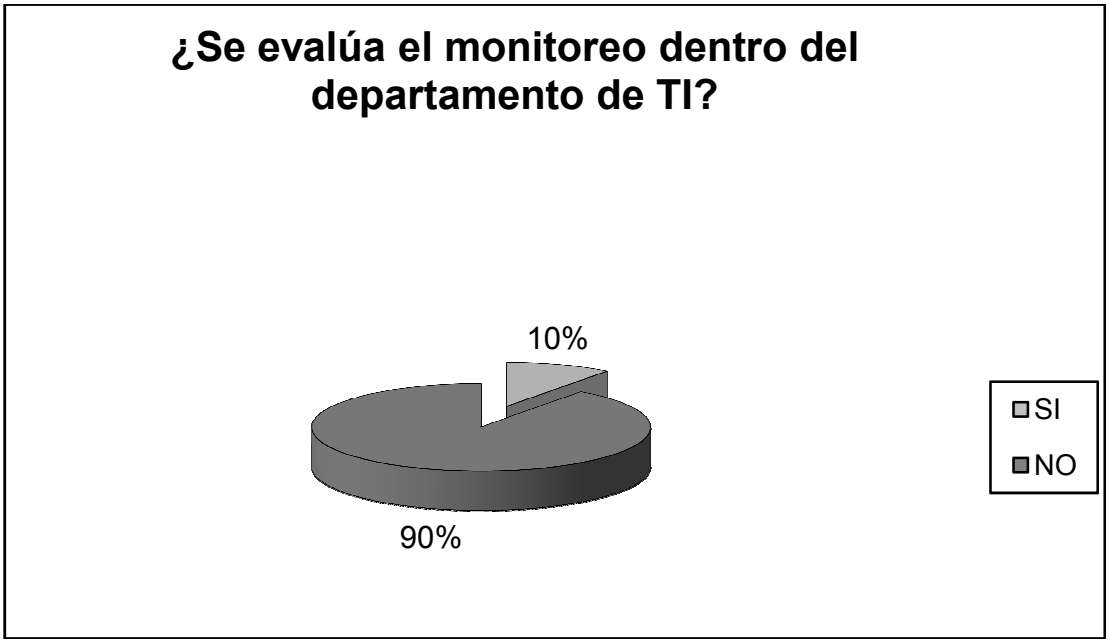


Figura 15. Detalle de planeación y organización

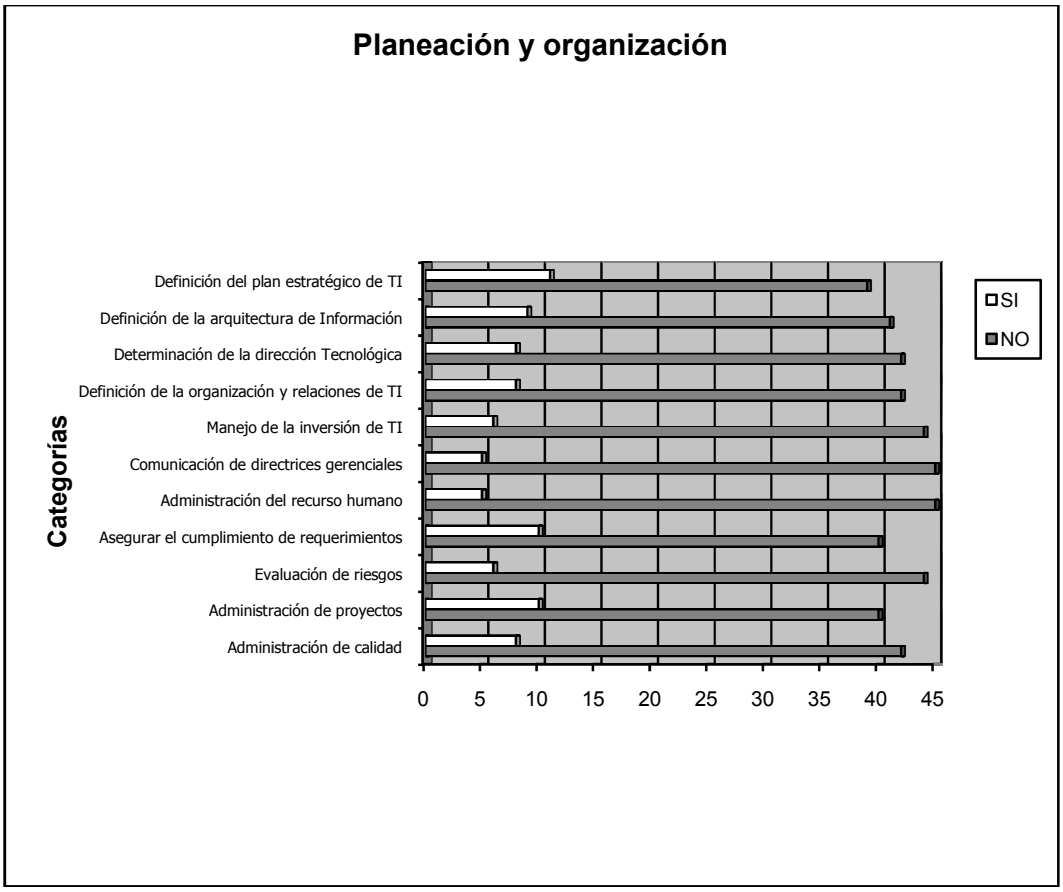


Figura 16. Detalle de adquisición e implementación

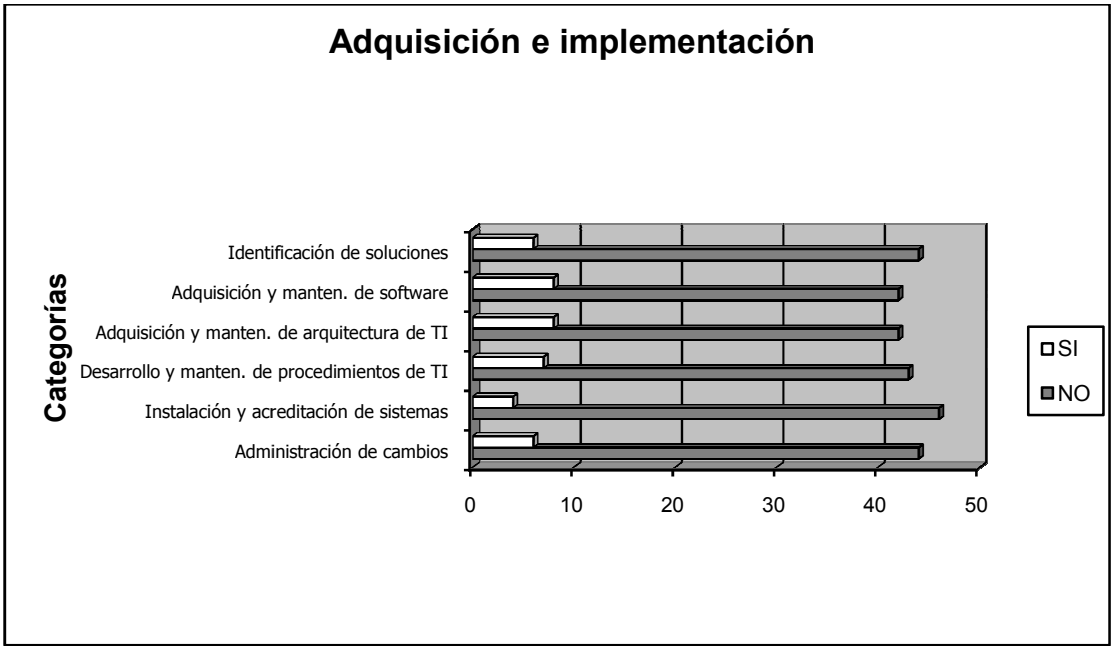


Figura 17. Detalle de monitoreo

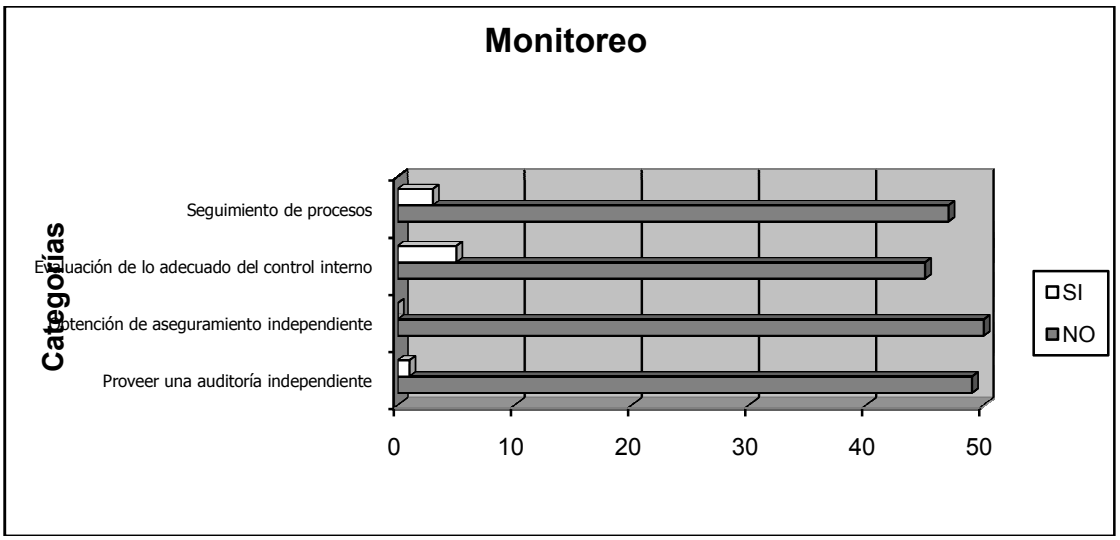
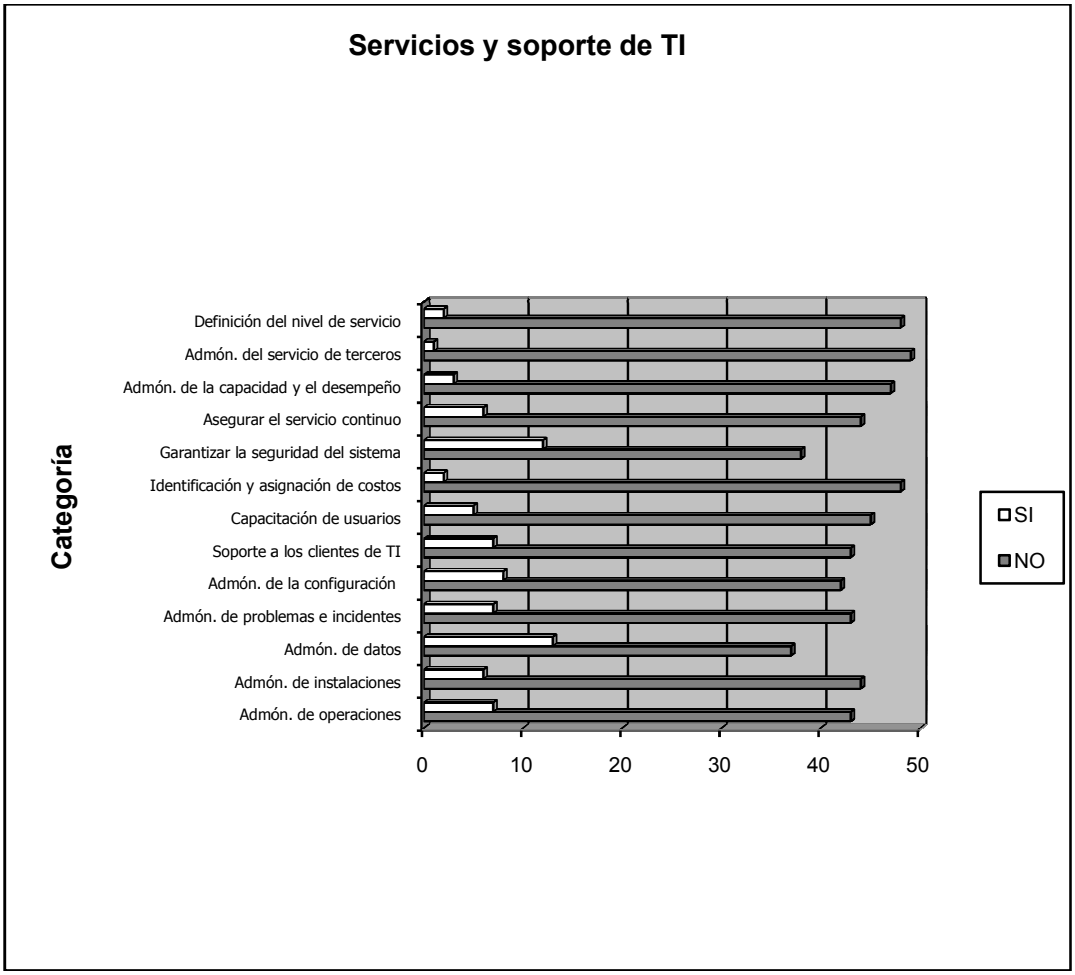


Figura 18. Detalle de servicios y soporte de TI


Servicios y soporte de TI
Categoría
Definición del nivel de servicio
Admón. del servicio de terceros
Admón. de la capacidad y el desempeño
Asegurar el servicio continuo
Garantizar la seguridad del sistema
Identificación y asignación de costos
Capacitación de usuarios
Soporte a los clientes de TI
Admón. de la configuración
Admón. de problemas e incidentes
Admón. de datos
Admón. de instalaciones
Admón. de operaciones
0
10
20
30
40
50
SI
NO

APÉNDICE B

El porcentaje de entendimiento con el que cuenta la alta dirección gerencial en los procesos del Departamento de TI, se puede establecer por medio de una encuesta, como la que se muestra a continuación:

1.- ¿Conoce la arquitectura de información e infraestructura con la que cuenta la empresa?

Muy bien	☐
Bien	☐
Poco	☐
Muy poco	☐
Nada	☐

2.- ¿Conoce los procesos y procedimientos que se utilizan en del Departamento de TI, para asegurar el cumplimiento de requerimientos y la calidad de los mismos?

Muy bien	☐
Bien	☐
Poco	☐
Muy poco	☐
Nada	☐

3.- ¿Conoce las políticas utilizadas para el desarrollo, instalación y administración de programas en el departamento de TI?

Muy bien	☐
Bien	☐
Poco	☐
Muy poco	☐
Nada	☐

4.- ¿Conoce cómo se garantiza la seguridad en los sistemas de información existentes?

Muy bien ☐

Bien ☐

Poco ☐

Muy poco ☐

Nada ☐

5.- ¿Conoce cuáles son los procedimientos y políticas del Departamento de TI, para asegurar el servicio continuo?

Muy bien ☐

Bien ☐

Poco ☐

Muy poco ☐

Nada ☐

6.- ¿En qué porcentaje de funcionamiento general conoce los sistemas de información que se utilizan en su empresa?

Muy bien ☐

Bien ☐

Poco ☐

Muy poco ☐

Nada ☐

7.- ¿Qué importancia significa la información de los sistemas informáticos en la toma de decisiones de la empresa?

Muy importante

Importante

Poco importarte

Muy poco

Nada

8.- ¿Conoce los proyectos existentes en el Departamento de TI y la administración de los mismos?

Muy bien

Bien

Poco

Muy poco

Nada

9.- ¿Cuál es el nivel de conocimiento que posee de los planes de contingencia en la recuperación de datos, problemas e incidentes?

Muy bien

Bien

Poco

Muy poco

Nada

10.- ¿Qué valor se le da en su empresa y cuál es el nivel de valor estratégico que se le da a los sistemas de información?

Muy bien

	☐
Bien	☐
Poco	☐
Muy poco	☐
Nada	☐

La forma de tabulación y determinación de porcentajes de las respuestas se realiza de la siguiente manera:

Muy bien	4pts.
Bien	3pts.
Poco	2pts.
Muy poco	1pts.
Nada	0pts.

De un total posible de 40 puntos, se deben sumar las respuestas con la ponderación antes mencionada, y determinar el porcentaje de conocimiento que se tiene de los procesos, procedimientos y sistemas del Departamento de TI, así como de la importancia que tienen los sistemas de información y datos, para el desempeño de la empresa.